~~TOP SECRET//COMINT//NOFORN//MR~~



UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, DC

IN RE PRODUCTION OF TANGIBLE THINGS FROM [redacted]

Docket Number: BR 08-13

**MEMORANDUM OF THE UNITED STATES IN RESPONSE TO THE COURT'S ORDER DATED JANAURY 28, 2009 (U)**

The United States of America, by and through the undersigned Department of Justice attorneys, respectfully submits this memorandum and supporting Declaration of Lt. General Keith B. Alexander, U.S. Army, Director, National Security Agency (NSA), attached hereto at Tab 1 ("Alexander Declaration"), in response to the Court's Order Regarding Preliminary Notice of Compliance Incident Dated January 15, 2009 ("January 28 Order"). ~~(TS)~~

The Government acknowledges that NSA's descriptions to the Court of the alert list process described in the Alexander Declaration were inaccurate and that the

~~TOP SECRET//COMINT//NOFORN//MR~~

[redacted]

Business Records Order did not provide the Government with authority to employ the alert list in the manner in which it did. ~~(TS//SI//NF)~~

For the reasons set forth below, however, the Court should not rescind or modify its Order in docket number BR 08-13. The Government has already taken significant steps to remedy the alert list compliance incident and has commenced a broader review of its handling of the metadata collected in this matter. In addition, the Government is taking additional steps to implement a more robust oversight regime. Finally, the Government respectfully submits that the Court need not take any further remedial action, including through the use of its contempt powers or by a referral to the appropriate investigative offices.[1] ~~(TS//SI//NF)~~

## BACKGROUND (U)

### I. Events Preceding the Court's January 28 Order ~~(S)~~

In docket number BR 06-05, the Government sought, and the Court authorized NSA, pursuant to the Foreign Intelligence Surveillance Act's (FISA) tangible things provision, 50 U.S.C. § 1861 et seq., to collect in bulk and on an ongoing basis certain call

[1] The January 28 Order directed the Government to file a brief to help the Court assess how to respond to this matter and to address seven specific issues. This memorandum discusses the need for further Court action based, in part, on the facts in the Alexander Declaration, which contains detailed responses to each of the Court's specific questions. See Alexander Decl. at 24-39. ~~(S)~~

detail records or "telephony metadata," so that NSA could analyze the metadata using contact chainin[redacted] tools.[2] ~~(TS//SI//NF)~~

FISA's tangible things provision authorizes the Director of the Federal Bureau of Investigation (FBI) or his designee to apply to this Court

> for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution.

50 U.S.C. § 1861(a)(1). FISA's tangible things provision directs the Court to enter an ex parte order requiring the production of tangible things and directing that the tangible things produced in response to such an order be treated in accordance with minimization procedures adopted by the Attorney General pursuant to section 1861(g), if the judge finds that the Government's application meets the requirements of 50 U.S.C. § 1861(a) & (b). See 50 U.S.C. § 1861(c)(1). (U)

In docket number BR 06-05 and each subsequent authorization, including docket number BR 08-13, this Court found that the Government's application met the requirements of 50 U.S.C. § 1861(a) & (b) and entered an order directing that the BR metadata to be produced—call detail records or telephony metadata—be treated in

[2] The Government will refer herein to call detail records collected pursuant to the Court's authorizations in this matter as "BR metadata." ~~(TS)~~

accordance with the minimization procedures adopted by the Attorney General.

Among these minimization procedures was the following:

> Any search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [redacted].[3] More specifically, access to the archived data shall occur only when NSA has identified a known telephone number for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] organization; provided, however, that a telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.

Order, docket number BR 06-05, at 5 (emphasis added); see also Memo. of Law in Supp. of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, docket number BR 06-05, Ex. C, at 20 (describing the above requirement as one of several minimization procedures to be applied to the collected metadata).[4] ~~(TS//SI//NF)~~

---

[3] Authorizations after this matter was initiated in May 2006 expanded the telephone identifiers that NSA could query to those identifiers associated with [redacted] see generally docket number BR 06-05 (motion to amend granted in August 2006), and later the [redacted], see generally docket number BR 07-10 (motion to amend granted in June 2007). The Court's authorization in docket number BR 08-13 approved querying related to [redacted] Primary Order, docket number BR 08-13, at 8. ~~(TS//SI//NF)~~

[4] In addition, the Court's Order in docket number BR 06-05 and each subsequent authorization, including docket number BR 08-13, required that "[a]lthough the data collected under this Order will necessarily be broad, the use of that information for analysis shall be strictly tailored to identifying terrorist communications and shall occur solely according to the

On December 11, 2008, the Court granted the most recent reauthorization of the BR metadata collection. For purposes of querying the BR metadata, as in prior Orders in this matter, the Court required the Government to comply with the same standard of reasonable, articulable suspicion set forth above. Primary Order, docket number BR 08-13, at 8-9.[5] ~~(TS//SI//NF)~~

On January 9, 2009, representatives from the Department of Justice's National Security Division (NSD) attended a briefing at NSA concerning the telephony metadata collection.[6] At the briefing, NSD and NSA representatives discussed several matters, including the alert list. See Alexander Decl. at 17, 27-28. Following the briefing and on the same day, NSD sent NSA an e-mail message asking NSA to confirm NSD's understanding of how the alert list operated as described at the briefing. Following additional investigation and the collection of additional information, NSA replied on

---

procedures described in the application, including the minimization procedures designed to protect U.S. person information." See, e.g., Order, docket number BR 06-05, at 6 ¶ D. ~~(TS//SI//NF)~~

[5] In this memorandum the Government will refer to this standard as the "RAS standard" and telephone identifiers that satisfy the standard as "RAS-approved." ~~(S)~~

[6] The names of the Department of Justice representatives who attended the briefing are included in the Alexander Declaration at page 28. The date of this meeting, January 9, 2009, was the date on which these individuals first learned (later confirmed) that the alert list compared non-RAS-approved identifiers to the incoming BR metadata. Other than these individuals (and other NSD personnel with whom these individuals discussed this matter between January 9 and January 15, 2009), and those NSA personnel otherwise identified in the Alexander Declaration, NSD has no record of any other executive branch personnel who knew that the alert list included non-RAS-approved identifiers prior to January 15, 2009. ~~(TS//SI//NF)~~

January 14, 2009, confirming much of NSD's understanding and providing some additional information. See id. at 27. ~~(TS//SI//NF)~~

Following additional discussions between NSD and NSA, a preliminary notice of compliance incident was filed with the Court on January 15, 2009. See id. at 27-28. The letter reported that the alert list contained counterterrorism-associated telephone identifiers tasked for collection pursuant to NSA's signals intelligence (SIGINT) authorities under Executive Order 12333, and therefore included telephone identifiers that were not RAS-approved, as well as some that were.[7] Thereafter, as previously reported in a supplemental notice of compliance incident filed with the Court on February 3, 2009, NSA unsuccessfully attempted to complete a software fix to the alert list process so that it comported with the above requirement in docket number BR 08-13.

---

[7] The preliminary notice of compliance incident filed on January 15, 2009, stated in pertinent part:

> NSA informed the NSD that NSA places on the alert list counterterrorism associated telephone identifiers that have been tasked for collection pursuant to NSA's signals intelligence (SIGINT) authorities under Executive Order 12333. Because the alert list consists of SIGINT-tasked telephone identifiers, it contains telephone identifiers as to which NSA has not yet determined that a reasonable and articulable suspicion exists that they are associated with [redacted] As information collected pursuant the Court's Orders in this matter flows into an NSA database, NSA automatically compares this information with its alert list in order to identify U.S. telephone identifiers that have been in contact with a number on the alert list. Based on results of this comparison NSA then determines in what body of data contact chaining is authorized.

Jan. 15, 2009, Preliminary Notice of Compliance Incident, docket number 08-13, at 2. ~~(TS//SI//NF)~~

See id. at 20. NSA shut down the alert list process entirely on January 24, 2009, and the process remains shut down as of the date of this filing.[8] See id. ~~(TS//SI//NF)~~

## II. NSA's Use of the Alert List Process to Query Telephony Metadata ~~(TS)~~

When the Court initially authorized the collection of telephony metadata in docket number BR 06-05 on May 24, 2006, neither the Court's Orders nor the Government's application (including the attachments) discussed an alert list process. Rather, a description of the alert list process first appeared in the NSA report accompanying the renewal application in BR 06-08, filed with the Court on August 18,

---

[8] The supplemental notice of compliance incident filed on February 3, 2009, stated in pertinent part:

> On January 23, 2009, NSA provided the NSD with information regarding the steps it had taken to modify the alert list process in order to ensure that only "RAS-approved" telephone identifiers run against the data collected pursuant to the Court's Orders in this matter (the "BR data") would generate automated alerts to analysts. Specifically, NSA informed the NSD that as of January 16, 2009, it had modified the alert list process so that "hits" in the BR data based on non-RAS-approved signals intelligence (SIGINT) tasked telephone identifiers would be automatically deleted so that only hits in the BR data based on RAS-approved telephone identifiers would result in an automated alert being sent to analysts. NSA also indicated that it was in the process of constructing a new alert list consisting of only RAS-approved telephone identifiers.
>
> On January 24, 2009, NSA informed the NSD that it had loaded to the business record alert system a different list of telephone identifiers than intended. NSA reports that, due to uncertainty as to whether all of the telephone identifiers satisfied all the criteria in the business records order, the alert list process was shut down entirely on January 24, 2009.

Feb. 3, 2009, Supplemental Notice of Compliance Incident, docket number 08-13, at 1-2. ~~(TS//SI//NF)~~

2006.[9] The reports filed with the Court incorrectly stated that the alert list did not include telephone identifiers that were not RAS-approved. In fact, the majority of telephone identifiers on the list were not RAS-approved. See Alexander Decl. at 4, 7-8. ~~(TS//SI//NF)~~

**A. Creation of the Alert List for BR Metadata in May 2006** ~~(TS)~~

Before the Court issued its Order in BR 06-05, NSA had developed an alert list process to assist NSA in prioritizing its review of the telephony metadata it received. See id. at 8. The alert list contained telephone identifiers NSA was targeting for SIGINT collection and domestic identifiers that, as a result of analytical tradecraft, were deemed relevant to the Government's counterterrorism activity. See id. at 9. The alert list process notified NSA analysts if there was a contact between either (i) a foreign telephone identifier of counterterrorism interest on the alert list and any domestic telephone identifier in the incoming telephony metadata, or (ii) any domestic telephone identifier on the alert list related to a foreign counterterrorism target and any foreign telephone identifier in the incoming telephony metadata. See id. ~~(TS//SI//NF)~~

According to NSA's review of its records and discussions with relevant NSA personnel, on May 25, 2006, NSA's Signals Intelligence Directorate (SID) asked for NSA Office of General Counsel's (OGC) concurrence on draft procedures for implementing

[9] Similarly, the applications and declarations in subsequent renewals did not discuss the alert list although the reports attached to the applications and reports filed separately from renewal applications discussed the process. ~~(TS)~~

the Court's Order in docket number BR 06-05. See id. at 12. The procedures generally described how identifiers on the alert list would be compared against incoming BR metadata and provided that a supervisor would be notified if there was a match between an identifier on the alert list and an identifier in the incoming data. See id. at 12-13 and Ex. B thereto ("BR Procedures") at 1-2. Moreover, a close reading of the BR Procedures indicated that the alert list contained both RAS-approved and non-RAS-approved telephone identifiers.[10] See Alexander Decl. at 12-13; BR Procedures at 1. NSA OGC concurred in the use of the BR Procedures, emphasizing that analysts could not access the archived BR metadata for purposes of conducting contact chaining [redacted] unless the RAS standard had been satisfied. See Alexander Decl. at 13-14 and Ex. A and Ex. B thereto. ~~(TS//SI//NF)~~

On May 26, 2006, the chief of NSA-Washington's counterterrorism organization in SID directed that the alert list be rebuilt to include only identifiers assigned to "bins" or "zip codes"[11] that NSA used to identify [redacted]

[10] For example, after describing the notification a supervisor (i.e., Shift Coordinator and, later, Homeland Mission Coordinator) would receive if a foreign telephone identifier generated an alert based on the alert list process, the BR Procedures provided that the "Shift Coordinator will examine the foreign number and determine if that particular telephone number has been previously associated w[redacted] based on the standard articulated by the Court." BR Procedures at 1. ~~(TS//SI//NF)~~

[redacted]

[redacted] the only targets of the Court's Order in docket number BR 06-05. See Alexander Decl. at 14-15. Pursuant to this overall direction, personnel in NSA's counterterrorism organization actually built two lists to manage the alert process. The first list — known as the "alert list" — included all identifiers (foreign and domestic) that were of interest to counterterrorism analysts who were charged with tracking [redacted] This list was used to compare the incoming BR metadata NSA was obtaining pursuant to the Court's Order and NSA's other sources of SIGINT collection to alert the counterterrorism organization if there was a match between a telephone identifier on the list and an identifier in the incoming metadata. See id. at 15. The alert list consisted of two partitions—one of RAS-approved identifiers that could result in automated chaining in the BR metadata and a second of non-RAS approved identifiers that could not be used to initiate automated chaining in the BR metadata. See id. The second list—known as the "station table"—was a historical listing of all telephone identifiers that had undergone a RAS determination, including the results of the determination. See id. at 15, 22. NSA used the "station table" to ensure that only RAS-approved "seed" identifiers were used to conduct chaining [redacted] in the BR metadata archive. See id. at 15. In short, the system was designed to compare both SIGINT and BR metadata against the identifiers on the alert list but only to permit

---

A chart of the alert list process as it operated from May 2006 to January 2009 is attached to the Alexander Declaration as Ex. C. ~~(S)~~

alerts generated from RAS-approved telephone identifiers to be used to conduct contact chaining [redacted] of the BR metadata. As a result, the majority of telephone identifiers compared against the incoming BR metadata in the rebuilt alert list were not RAS-approved. See id. at 4, 7-8. For example, as of January 15, 2009, the date of NSD's first notice to the Court regarding this issue, only 1,935 of the 17,835 identifiers on the alert list were RAS-approved. See id. at 8. ~~(TS//SI//NF)~~

Based upon NSA's recent review, neither NSA SID nor NSA OGC identified the inclusion of non-RAS-approved identifiers on the alert list as an issue requiring extensive analysis. See id. at 11. Moreover, NSA personnel, including the OGC attorney who reviewed the BR Procedures, appear to have viewed the alert process as merely a means of identifying a particular identifier on the alert list that might warrant further scrutiny, including a determination of whether the RAS standard had been satisfied and therefore whether contact chaining [redacted] could take place in the BR metadata archive using that particular identifier.[12] See id. at 11-12. In fact, NSA designed the alert list process to result in automated chaining of the BR metadata only if the initial alert was based on a RAS-approved telephone identifier. See id. at 14. If an

[12] As discussed in the Alexander Declaration, in the context of NSA's SIGINT activities the term "archived data" normally refers to data stored in NSA's analytical repositories and excludes the many processing steps NSA undertakes to make the raw collections useful to analysts. Accordingly, NSA analytically distinguished the initial alert process from the subsequent process of performing contact chaining [redacted] (i.e., "queries") of the "archived data," assessing that the Court's Order in docket number BR 06-05 only governed the latter. See Alexander Decl. at 3-4, 10-15. ~~(TS//SI//NF)~~

alert was based on a non-RAS-approved identifier, no automated chaining would occur in the BR metadata archive although automated chaining could occur in other NSA archives that did not require a RAS determination (e.g., non-FISA telephony collection). See id. ~~(TS//SI//NF)~~

**B. Description of the Alert List Process Beginning in August 2006 ~~(TS)~~**

The first description of the alert list process appeared in the NSA report accompanying the Government's renewal application filed with the Court on August 18, 2006. The report stated in relevant part:

> ~~(TS//SI//NF)~~ NSA has compiled through its continuous counter-terrorism analysis, a list of telephone numbers that constitute an "alert list" of telephone numbers used by members of [redacted] This alert list serves as a body of telephone numbers employed to query the data, as is described more fully below.
>
> ~~(TS//SI//NF)~~ Domestic numbers and foreign numbers are treated differently with respect to the criteria for including them on the alert list. With respect to foreign telephone numbers, NSA receives information indicating a tie to [redacted] Principal among these are: [redacted] Each of the foreign telephone numbers that comes to the attention of NSA as possibly related to [redacted] is evaluated to determine whether the information about it provided to NSA satisfies the reasonable articulable suspicion standard. If so, the foreign telephone number is placed on the alert list; if not, it is not placed on the alert list.
>
> ~~(TS//SI//NF)~~ The process set out above applies also to newly discovered domestic telephone numbers considered for addition to the

> alert list, with the additional requirement that NSA's Office of General Counsel reviews these numbers and affirms that the telephone number is not the focus of the analysis based solely on activities that are protected by the First Amendment. . . .
>
> . . . .
>
> ~~(TS//SI//NF)~~ As of the last day of the reporting period addressed herein, NSA had included a total of 3980 telephone numbers on the alert list, which includes foreign numbers and domestic numbers, after concluding that each of the foreign telephone numbers satisfied the standard set forth in the Court's May 24, 2006 [Order], and each of the domestic telephone numbers was either a FISC approved number or in direct contact with a foreign seed that met those criteria.
>
> ~~(TS//SI//NF)~~ To summarize the alert system: every day new contacts are automatically revealed with the 3980 telephone numbers contained on the alert list described above, which themselves are present on the alert list either because they satisfied the reasonable articulable suspicion standard, or because they are domestic numbers that were either a FISC approved number or in direct contact with a number that did so. These automated queries identify any new telephone contacts between the numbers on the alert list and any other number, except that domestic numbers do not alert on domestic-to-domestic contacts.

NSA Report to the FISC (Aug. 18, 2006), docket number BR 06-05 (Ex. B to the Government's application in docket number BR 06-08), at 12-15 ("August 2006 Report").[13] The description above was included in similar form in all subsequent reports to the Court, including the report filed in December 2008. ~~(TS//SI//NF)~~

[13] The August 2006 report also discussed two categories of domestic telephone numbers that were added to the alert list prior to the date the Order took effect. One category consisted of telephone numbers for which the Court had authorized collection and were therefore deemed approved for metadata querying without the approval of an NSA official. The second category consisted of domestic numbers added to the alert list after direct contact with a known foreign [redacted] seed number. The domestic numbers were not used as seeds themselves and contact chaining was limited to two hops (instead of the three hops authorized by the Court). See August 2006 Report, at 12-13; Alexander Decl. at 2 n.1. NSA subsequently removed the numbers in the second category from the alert list. ~~(TS//SI//NF)~~

According to NSA's review of its records and discussions with relevant NSA personnel, the NSA OGC attorney who prepared the initial draft of the report included an inaccurate description of the alert list process due to a mistak[redacted]lert [redacted] Upon completing the draft, the attorney circulated the draft to other OGC attorneys and operational personnel and requested that others review it for accuracy. See id. The inaccurate description, however, was not corrected before the report was finalized and filed with the Court on August 18, 2006. The same description remained in subsequent reports to the Court, including the report filed in docket number BR 08-13.[14] ~~(TS//SI//NF)~~

[14] At the meeting on January 9, 2009, NSD and NSA also identified that the reports filed with the Court have incorrectly stated the number of identifiers on the alert list. Each report included the number of telephone identifiers purportedly on the alert list. See, e.g., NSA 120-Day Report to the FISC (Dec. 11, 2008), docket number BR 08-08 (Ex. B to the Government's application in docket number BR 08-13), at 11 ("As of November 2, 2008, the last day of the reporting period herein, NSA had included a total of 27,090 telephone identifiers on the alert list . . . ."). In fact, NSA reports that these numbers did not reflect the total number of identifiers on the alert list; they actually represented the total number of identifiers included on the "station table" (NSA's historical record of RAS determinations) as currently RAS-approved (i.e., approved for contact chaining[redacted]. See Alexander Decl. at 8 n.3. ~~(TS//SI//NF)~~

## DISCUSSION (U)

## I. THE COURT'S ORDERS SHOULD NOT BE RESCINDED AND NEED NOT BE MODIFIED ~~(TS)~~

In the January 28 Order, the Court directed the Government to submit a written brief designed to, among other things, assist the Court in assessing whether the Primary Order in docket number BR 08-13 should be modified or rescinded.[15] January 28 Order at 2. ~~(S)~~

So long as a court retains jurisdiction over a case, then, in the absence of a prohibition by statute or rule, the court retains inherent authority to "reconsider, rescind, or modify an interlocutory order for cause seen by it to be sufficient." Melancon v. Texaco, Inc., 659 F.3d 551, 553 (5th Cir. 1981). The choice of remedies rests in a court's sound discretion, see Kingsley v. United States, 968 F.2d 109, 113 (1st Cir. 1992) (citations omitted) (considering the alternative remedies for breach of a plea agreement), but in exercising that discretion a court may consider the full consequences that a particular remedy may bring about, see Alrefae v. Chertoff, 471 F.3d 353, 360 (2d Cir. 2006) (citations omitted) (instructing that on remand to consider petitioner's motion to rescind order of removal, immigration judge may consider "totality of the circumstances"). Consonant with these principles, prior decisions of this Court reflect a strong preference for resolving incidents of non-compliance through the creation of

[15] The authorization granted by the Primary Order issued by the Court in docket number BR 08-13 expires on March 6, 2009 at 5:00 p.m. Eastern Time. ~~(TS//SI//NF)~~

additional procedures and safeguards to guide the Government in its ongoing collection efforts, rather than by imposing the extraordinary and final remedy of rescission. See, e.g., [redacted], Primary Order, docket numbe[redacted] at 11-12 (requiring, in response to an incident of non-compliance, NSA to file with the Court every thirty days a report discussing, among other things, queries made since the last report to the Court and NSA's application of the relevant standard); see also [redacted] docket numbers [redacted] (prohibiting the querying of data using "seed" accounts validated using particular information). ~~(TS//SI//NF)~~

The Court's Orders in this matter did not authorize the alert list process as implemented to include a comparison of non-RAS-approved identifiers against incoming BR metadata. However, in light of the significant steps that the Government has already taken to remedy the alert list compliance incident and its effects, the significant oversight modifications the Government is in the process of implementing, and the value of the telephony metadata collection to the Government's national security mission, the Government respectfully submits that the Court should not rescind or modify the authority granted in docket number BR 08-13. ~~(TS)~~

### A. Remedial Steps Already Undertaken by the Government Are Designed to Ensure Future Compliance with the Court's Orders and to Mitigate Effects of Past Non-Compliance (S)

Since the Government first reported this matter to the Court, NSA has taken several corrective measures related to the alert process, including immediate steps to sequester and shut off its analysts' access to any alerts that were generated from comparing incoming BR metadata against non-RAS-approved identifiers. See Alexander Decl. at 19-20. NSA also immediately began to re-engineer the entire alert process to ensure that only RAS-approved telephone identifiers are compared against incoming BR metadata. See id. Most importantly, NSA shut off the alert list process on January 24, 2009, when its redesign efforts failed, and the process will remain shut down until the Government can ensure that the process will operate within the terms of the Court's Orders. See id. at 20. ~~(TS//SI//NF)~~

NSA has also conducted a review of all 275 reports NSA has disseminated since May 2006 as a result of contact chaining [redacted] of NSA's archive of BR metadata.[16] See id. at 36. Thirty-one of these reports resulted from the automated alert process. See id. at 36 n.17. NSA did not identify any report that resulted from the use of a non-RAS-approved "seed" identifier.[17] See id. at 36-37. Additionally, NSA

---

[16] A single report may tip more than one telephone identifier as being related to the seed identifier. As a result, the 275 reports have tipped a total of 2,549 telephone identifiers since May 24, 2006. See Alexander Decl. at 36 n.17. ~~(TS//SI//NF)~~

[17] NSA has identified one report where the number on the alert list was not RAS-approved when the alert was generated but, after receiving the alert, a supervisor determined

determined that in all instances where a U.S. identifier served as the initial seed identifier for a report (22 of the 275 reports), the initial U.S. seed identifier was either already the subject of FISC-approved surveillance under the FISA or had been reviewed by NSA's OGC to ensure that the RAS determination was not based solely on a U.S. person's first amendment-protected activities. See id. at 37. ~~(TS//SI//NF)~~

Unlike reports generated from the BR metadata, which NSA disseminated outside NSA, the alerts generated from a comparison of the BR metadata to the alert list were only distributed to NSA SIGINT personnel responsible for counterterrorism activity.[18] See id. at 38. Since this compliance incident surfaced, NSA identified and eliminated analyst access to all alerts that were generated from the comparison of non-RAS approved identifiers against the incoming BR metadata and has limited access to the BR alert system to only software developers assigned to NSA's Homeland Security Analysis Center (HSAC), and the Technical Director for the HSAC. See id. at 38-39. ~~(TS//SI//NF)~~

---

that the identifier, in fact, satisfied the RAS standard. After this determination, NSA used the identifier as a seed for chaining in the BR FISA data archive. Information was developed that led to a report to the FBI that tipped 11 new telephone identifiers. See Alexander Decl. at 37 n.18. ~~(TS//SI//NF)~~

[18] Initially, if an identifier on the alert list generated an alert that the identifier had been in contact with an identifier in the United States, the alert system masked (i.e., concealed from the analyst's view) the domestic identifier. Later, in January 2008, the SIGINT Directorate allowed the alerts to be sent to analysts without masking the domestic identifier. NSA made this change in an effort to improve the ability of SIGINT analysts, on the basis of their target knowledge, to prioritize their work more efficiently. See Alexander Decl. at 38. ~~(TS//SI//NF)~~

In addition to the steps NSA has taken with respect to the alert list issues, NSA has also implemented measures to review NSA's handling of the BR metadata generally. For example, the Director of NSA has ordered end-to-end system engineering and process reviews (technical and operational) of NSA's handling of BR metadata. See id. at 21. The results of this review will be made available to the Court. See id. at 21 n.13. In response to this Order, NSA also has undertaken the following:

- a review of domestic identifiers on the "station table" in order to confirm that RAS determinations complied with the Court's Orders; and
- an audit of all queries made of the BR metadata repository since November 1, 2008, to determine if any of the queries during that period were made using non-RAS-approved identifiers.[19]

See id. at 22-23. ~~(TS//SI//NF)~~

To better ensure that NSA operational personnel understand the Court-ordered procedures and requirements for accessing the BR metadata, NSA's SIGINT Oversight & Compliance Office also initiated an effort to redesign training for operational personnel who require access to BR metadata. This effort will include competency testing prior to access to the data. See id. at 23. In the interim, NSA management personnel, with support from NSA OGC and the SIGINT Oversight and Compliance Office, delivered

[19] Although NSA's review is still ongoing, NSA's review to date has revealed no instances of improper querying of the BR metadata, aside from those previously reported to the Court in a notice of compliance incident filed on January 26, 2009, in which it was reported that between approximately December 10, 2008, and January 23, 2009, two analysts conducted 280 queries using non-RAS-approved identifiers. See Alexander Decl. at 22-23. As discussed below, NSA is implementing software changes to the query tools used by analysts so that only RAS-approved identifiers may be used to query the BR FISA data repository. See id. at 22-23. ~~(TS)~~

in-person briefings for all NSA personnel who have access to the BR metadata data archive to remind them of the requirements and their responsibilities regarding the proper handling of BR metadata. See id. In addition, all NSA personnel with access to the BR metadata have also received a written reminder of their responsibilities. See id. ~~(TS//SI//NF)~~

Finally, NSA is implementing two changes to the tools used by analysts to access the BR metadata. First, NSA is changing the system that analysts use to conduct contact chaining of the BR metadata so that the system will not be able to accept any non-RAS-approved identifier as the seed identifier for contact chaining. See id. at 24. Second, NSA is implementing software changes to its system that will limit to three the number of "hops" permitted from a RAS-approved seed identifier. See id. ~~(TS//SI//NF)~~

**B. Additional Oversight Mechanisms the Government Will Implement ~~(S)~~**

The operation of the alert list process in a manner not authorized by the Court and contrary to the manner in which it was described to the Court is a significant compliance matter. While the process has been remedied in the ways described above, the Government has concluded that additional oversight mechanisms are appropriate to ensure future compliance with the Primary Order in docket number BR 08-13 and any future orders renewing the authority granted therein. Accordingly, the Government will implement the following oversight mechanisms in addition to those contained in the Court's Orders:

- NSA's OGC will consult with NSD on all significant legal opinions that relate to the interpretation, scope and/or implementation of the authorization granted by the Court in its Primary Order in docket number BR 08-13, prior Orders issued by the Court, or any future order renewing that authorization. When operationally practicable, such consultation shall occur in advance; otherwise NSD will be notified as soon as practicable;
- NSA's OGC will promptly provide NSD with copies of the mandatory procedures (and all replacements, supplements or revisions thereto in effect now or adopted in the future) the Director of NSA is required to maintain to strictly control access to and use of the data acquired pursuant to orders issued by the Court in this matter;
- NSA's OGC will promptly provide NSD with copies of all formal briefing and/or training materials (including all revisions thereto) currently in use or prepared and used in the future to brief/train NSA personnel concerning the authorization granted by orders issued by the Court in this matter;
- At least once before any future orders renewing the authorization granted in docket number BR 08-13 expire, a meeting for the purpose of assessing compliance with this Court's orders will be held with representatives from NSA's OGC, NSD, and appropriate individuals from NSA's Signals Intelligence Directorate. The results of this meeting will be reduced to writing and submitted to the Court as part of any application to renew or reinstate this authority;
- At least once during the authorization period of all future orders, NSD will meet with NSA's Office of Inspector General (OIG) to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders in this matter;
- Prior to implementation, all proposed automated query processes will be reviewed and approved by NSA's OGC and NSD.

~~(TS//SI//NF)~~

While no oversight regime is perfect, the Government submits that this more robust oversight regime will significantly reduce the likelihood of such compliance incidents occurring in the future. ~~(TS)~~

C. The Value of the BR Metadata to the Government's National Security Mission ~~(TS)~~

The BR metadata plays a critical role in the Government's ability to find and identify members and agents of [redacted]. As discussed in declarations previously filed with the Court in this matter, operatives of [redacted]s use the international telephone system to communicate with one another between numerous countries all over the world, including to and from the United States. Access to the accumulated pool of BR metadata is vital to NSA's counterterrorism intelligence mission because it enables NSA to discover the communications of these terrorist operatives. See Alexander Decl. at 39-42. While terrorist operatives often take intentional steps to disguise and obscure their communications and their identities using a variety of tactics, by employing its contact chaining [redacted] against the accumulated pool of metadata NSA can discover valuable information about the adversary. See id. Specifically, using contact chaining [redacted] NSA may be able to discover previously unknown telephone identifiers used by a known terrorist operative, to discover previously unknown terrorist operatives, to identify hubs or common contacts between targets of interest who were previously thought to be unconnected, and potentially to discover individuals willing to become U.S. Government assets. See, e.g., Decl. of Lt. Gen. Keith B. Alexander, docket number BR 06-05, Ex. A at ¶ 9; Decl. of [redacted] docket

number BR 08-13, Ex. A at ¶¶ 9-11.[20] Such discoveries are not possible when targeting solely known terrorist telephone identifiers. See Alexander Decl. at 39-40. Demonstrating the value of the BR metadata to the U.S. Intelligence Community, the NSA has disseminated 275 reports and tipped over 2,500 telephone identifiers to the FBI and CIA for further investigative action since the inception of this collection in docket number BR 06-05. See id. at 42. This reporting has provided the FBI with leads and linkages on individuals in the U.S. with connections to terrorism that it may have otherwise not identified. See id. ~~(TS//SI//NF)~~

In summary, the unquestionable foreign intelligence value of this collection, the substantial steps NSA has already taken to ensure the BR metadata is only accessed in compliance with the Court's Orders, and the Government's enhanced oversight regime provide the Court with a substantial basis not to rescind or modify the authorization for this collection program. ~~(TS)~~

## III. THE COURT NEED NOT TAKE ADDITIONAL ACTION REGARDING MISREPRESENTATIONS THROUGH ITS CONTEMPT POWERS OR BY REFERRAL TO APPROPRIATE INVESTIGATIVE OFFICES ~~(TS)~~

The January 28 Order asks "whether the Court should take action regarding persons responsible for any misrepresentation to the Court or violation of its Orders,

---

[20] Other advantages of contact chaining include [redacted]. See Alexander Decl. at 41; Decl. of [redacted] docket number BR 08-13, Ex. A at ¶ 10. ~~(TS//SI//NF)~~

either through its contempt powers or by referral to the appropriate investigative offices." January 28 Order at 2. The Government respectfully submits that such actions are not required. Contempt is not an appropriate remedy on these facts, and no referral is required, because NSA already has self-reported this matter to the proper investigative offices. ~~(TS//SI//NF)~~

Whether contempt is civil or criminal in nature turns on the "character and purpose" of the sanction involved. See Int'l Union, United Mine Workers of Am. v. Bagwell, 512 U.S. 821, 827 (1994) (quoting Gompers v. Bucks Stove & Range Co., 221 U.S. 418, 441 (1911)). Criminal contempt is punitive in nature and is designed to vindicate the authority of the court. See Bagwell, 512 U.S. at 828 (internal quotations and citations omitted). It is imposed retrospectively for a "completed act of disobedience," and has no coercive effect because the contemnor cannot avoid or mitigate the sanction through later compliance. Id. at 828-29 (citations omitted).[21] Because NSA has stopped the alert list process and corrected the Agency's unintentional misstatements to the Court, any possible contempt sanction here would be in the nature of criminal contempt. ~~(TS//SI//NF)~~

[21] By contrast, civil contempt is "remedial, and for the benefit of the complainant." Gompers, 221 U.S. at 441. It "is ordinarily used to compel compliance with an order of the court," Cobell v. Norton, 334 F.3d 1128, 1145 (D.C. Cir. 2003), and may also be designed "to compensate the complainant for losses sustained." United States v. United Mine Workers of America, 330 U.S. 258, 303-04 (1947) (citations omitted). (U)

A finding of criminal contempt "requires both a contemptuous act and a wrongful state of mind." Cobell, 334 F.3d at 1147 (citations omitted). The violation of the order must be willful: "a volitional act by one who knows or should reasonably be aware that his conduct is wrongful." United States v. Greyhound Corp., 508 F.2d 529, 531-32 (7th Cir. 1974), quoted in In re Holloway, 995 F.2d 1080, 1082 (D.C. Cir. 1993) (emphasis in original). For example, a criminal contempt conviction under 18 U.S.C. § 401 requires, among other things, proof of a willful violation of a court order; i.e., where the defendant "acts with deliberate or reckless disregard of the obligations created by a court order." United States v. Rapone, 131 F.3d 188, 195 (D.C. Cir. 1997) (citations omitted).[22] (U)

Here, there are no facts to support the necessary finding that persons at NSA willfully violated the Court's Orders or intentionally sought to deceive the Court. To the contrary, NSA operational personnel implemented the alert list based on the concurrence of its OGC to a set of procedures that contemplated comparing the alert list, including non-RAS-approved telephone identifiers, against a flow of new BR metadata. See Alexander Decl. at 12-14. The concurrence of NSA's OGC was based on NSA's understanding that, by using the term "archived data," the Court's Order in

[22] A person charged with contempt committed out of court is entitled to the usual protections of criminal law, such as the presumption of innocence and the right to a jury trial. Bagwell, 512 U.S. at 827-28. For criminal contempt to apply, a willful violation of an order must be proved beyond a reasonable doubt. See id. Contempt occurring in the presence of the Court, however, is not subject to all such protections. See id. at 827 n.2. (U)

docket number BR 06-05 only required the RAS standard to be applied to the contact chaining [redacted] conducted by accessing NSA's analytic repository of BR metadata. See id. at 10-14. This advice was given for the purpose of advising NSA operators on how to comply with the Court's Orders when using an alert list. Its goal plainly was not to deliberately or recklessly disregard those Orders; and in heeding this advice, NSA operators were not themselves seeking to deliberately or recklessly disregard the Court's Orders. Indeed, the NSA attorney who reviewed the procedures added language to the procedures to emphasize the Court's requirement that the RAS standard must be satisfied prior to conducting any chaining [redacted] of NSA's analytic repository of BR metadata. See id. at 13-14. ~~(TS//SI//NF)~~

NSA OGC's concurrence on the procedures the SIGINT Directorate developed for processing BR metadata also established the framework for numerous subsequent decisions and actions, including the drafting and reviewing of NSA's reports to the Court. NSA personnel reasonably believed, based on NSA OGC's concurrence with the BR Procedures, that the queries subject to the Court's Order were only contact chaining [redacted] of the aggregated pool of BR metadata. Against this backdrop, NSA operational personnel reasonably believed that, until contact chaining of the aggregated pool of BR metadata was conducted, the alert list process was not subject to the RAS requirement contained in the Court's Order. This, in turn, led to the misunderstanding between the NSA attorney who prepared the initial draft of NSA's

first BR report to the Court and the individual in the SIGINT Directorate who served as the report's primary reviewer, so that ultimately the report contained an incorrect description of the alert list process. See id. at 16-18.[23] In other words, there was no deliberate effort to provide inaccurate or misleading information to the Court, nor did any NSA employee deliberately circumvent the RAS requirement contained in the Court's Orders. Based on this confluence of events, all parties involved in the drafting of the report believed the description of the alert list to be accurate. ~~(TS//SI//NF)~~

In addition, the Government has already taken steps to notify the appropriate investigative officials regarding this matter. Specifically, FBI's OGC was informed of this matter on January 23, 2009; the Director of National Intelligence was informed of this matter on January 30, 2009, and received additional information about the incident on two other occasions; and the Undersecretary of Defense for Intelligence was informed of this matter on February 10, 2009. See id. at 28-29. NSA has also notified its Inspector General of this matter. See id. at 28. Finally, NSA is in the process of formally reporting this matter to the Assistant Secretary of Defense for Intelligence Oversight and subsequently the President's Intelligence Oversight Board. See id. at 28-29. (S)

---

[23] As described above, the alert list actually consisted of two partitions—one of RAS-approved identifiers that could result in automated chaining in the BR metadata and a second of non-RAS approved identifiers that could not be used to initiate automated chaining in the BR metadata. See Alexander Decl. at 15. ~~(TS//SI//NF)~~

## CONCLUSION (U)

For the reasons provided above, while the Government acknowledges that its descriptions of the alert list process to the Court were inaccurate and that the Court's Orders in this matter did not authorize the alert list process as implemented, the Court should not rescind or modify its Order in docket number BR 08-13 or take any further remedial action. ~~(TS//SI//NF)~~

Respectfully submitted,

Matthew G. Olsen
Acting Assistant Attorney General

[redacted]
Office of Intelligence

National Security Division
United States Department of Justice

1

~~TOP SECRET//COMINT//NOFORN//MR~~

**UNITED STATES**
**FOREIGN INTELLIGENCE SURVEILLANCE COURT**
**WASHINGTON, D.C.**

| | |
|---|---|
| (TS) In Re Production of Tangible Things from [redacted] | Docket No.: BR 08-13 |

**DECLARATION OF LIEUTENANT GENERAL KEITH B. ALEXANDER, UNITED STATES ARMY, DIRECTOR OF THE NATIONAL SECURITY AGENCY**

(U) I, Lieutenant General Keith B. Alexander, depose and state as follows:

(U) I am the Director of the National Security Agency ("NSA" or "Agency"), an intelligence agency within the Department of Defense ("DoD"), and have served in this position since 2005. I currently hold the rank of Lieutenant General in the United States Army and, concurrent with my current assignment as Director of the National Security Agency, I also serve as the Chief of the Central Security Service and as the Commander of the Joint Functional Component Command for Network Warfare. Prior to my current assignment, I have held other senior supervisory positions as an officer of the United States military, to include service as the Deputy Chief of Staff (DCS, G-2), Headquarters, Department of the Army; Commander of the US Army's Intelligence and Security Command; and the Director of Intelligence, United States Central Command.



[redacted]

(S) As the Director of the National Security Agency, I am responsible for directing and overseeing all aspects of NSA's cryptologic mission, which consists of three functions: to engage in signals intelligence ("SIGINT") activities for the US Government, to include support to the Government's computer network attack activities; to conduct activities concerning the security of US national security telecommunications and information systems; and to conduct operations security training for the US Government. Some of the information NSA acquires as part of its SIGINT mission is collected pursuant to Orders issued under the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA").

(U) The statements herein are based upon my personal knowledge, information provided to me by my subordinates in the course of my official duties, advice of counsel, and conclusions reached in accordance therewith.

**I. (U) Purpose:**

~~(S//SI//NF)~~ This declaration responds to the Court's Order of 28 January 2009 ("BR Compliance Order"), which directed the Government to provide the Foreign Intelligence Surveillance Court ("FISC" or "Court") with information "to help the Court assess whether the Orders issued in this docket should be modified or rescinded; whether other remedial steps should be directed; and whether the Court should take action regarding persons responsible for any misrepresentations to the Court or violations of its Orders, either through its contempt powers or by referral to appropriate investigative offices."

~~(S//NF)~~ To this end, this declaration describes the compliance matter that gave rise to the BR Compliance Order; NSA's analysis of the underlying activity; the root causes of the compliance problem; the corrective actions NSA has taken and plans to take to avoid a reoccurrence of the incident; answers to the seven (7) specific questions the Court has asked regarding the incident; and a description of the importance of this collection to the national security of the United States.

## II. (U) Incident:

### A. (U) Summary

~~(TS//SI//NF)~~ Pursuant to a series of Orders issued by the Court since May 2006, NSA has been receiving telephony metadata from telecommunications providers. NSA refers to the Orders collectively as the "Business Records Order" or "BR FISA." With each iteration of the Business Records Order, the Court has included language which says "access to the *archived data* shall occur only when NSA has identified a known telephone identifier for which . . . there are facts giving rise to a reasonable articulable suspicion that the telephone identifier is associated with [redacted] *See, e.g.,* Docket BR 08-13, Primary Order, 12 December 2008, *emphasis added.* For reasons described in more detail in the Section III.A. of this declaration, NSA personnel understood the term "archived data" to refer to NSA's analytic repository of BR FISA metadata and implemented the Business Records Order accordingly.

~~(TS//SI//NF)~~ While NSA did not authorize contact chaining [redacted] to occur in the Agency's analytic repository of BR FISA material unless NSA had determined that the "seed" telephone identifier for the chaining [redacted] satisfied the reasonable articulable suspicion ("RAS") standard specified in the Order, in its reports to the Court regarding NSA's implementation of the Business Records Order, the Agency incorrectly described an intermediate step called the alert process that NSA applied to the incoming stream of BR FISA metadata. The alert process would notify counterterrorism (CT) analysts if a comparison of the incoming metadata NSA was receiving from the Business Records Order and other sources of SIGINT collection revealed a match with telephone identifiers that were on an alert list of identifiers that were already of interest to CT personnel.

~~(TS//SI//NF)~~ In its reports to the Court, NSA stated the alert list only contained telephone identifiers that satisfied the RAS standard. In reality, the majority of identifiers on the alert list were CT identifiers that had not been assessed for RAS. If one of these non-RAS approved identifiers generated an alert, a CT analyst was notified so that NSA could make a RAS determination. If the Agency determined the identifier satisfied the RAS standard, only then would the identifier be approved as a seed for contact chaining [redacted] in the Agency's BR FISA analytic repository (*i.e.*, the "archived data"). If the contact chaining [redacted] produced information of foreign intelligence value, an NSA analyst would issue a report. In other words, none of NSA's BR FISA reports were based on non-RAS approved identifiers across the period in question – May 2006 through January 2009.

~~(S//SI)~~ I wish to emphasize that neither I nor the Agency is attempting to downplay the significance of NSA's erroneous description of the alert process to the Court. In retrospect, the Business Records Order did not provide NSA with specific authority to employ the alert list in the manner in which it did. The Agency's failure to describe the alert process accurately to the Court unintentionally precluded the Court from determining for itself whether NSA was correctly implementing the Court's Orders. Although I do not believe that any NSA employee intended to provide inaccurate or misleading information to the Court, I fully appreciate the severity of this error.

**B. (U) Details**

~~(TS//SI//NF)~~ Docket BR 08-13 is the FISC's most recent renewal of authority first granted to the Government in May 2006 to receive access to business records in the form of telephone call detail records. *See* Docket BR 06-05, 24 May 2006. NSA developed the automated alert process to notify NSA analysts of contact between a foreign telephone identifier of counterterrorism interest and any domestic telephone identifier; or any contact between a domestic telephone identifier, related to a foreign counterterrorism target, and any foreign telephone identifier. In its first BR FISA report to the Court in August 2006, the Agency described the automated alert process as follows:

> ~~(TS//SI//NF)~~ NSA has compiled through its continuous counter-terrorism analysis, a list of telephone numbers that constitute an "alert list" of telephone numbers used by members of [redacted]. This alert list serves as a body of telephone numbers employed to query the data, as is described more fully below.
>
> ~~(TS//SI//NF)~~ Domestic numbers and foreign numbers are treated differently with respect to the criteria for including them on the alert list.

With respect to foreign telephone numbers, NSA receives information indicating a tie to [redacted] from a variety of sources. Principal among these are: [redacted] Each of the foreign telephone numbers that comes to the attention of NSA as possibly related to [redacted] is evaluated to determine whether the information about it provided to NSA satisfies the reasonable articulable suspicion standard. If so, the foreign telephone number is placed on the alert list; if not, it is not placed on the alert list.

~~(TS//SI//NF)~~ The process set out above applies also to newly discovered domestic telephone numbers considered for addition to the alert list, with the additional requirement that NSA's Office of General Counsel reviews these numbers and affirms that the telephone number is not the focus of the analysis based solely on activities that are protected by the First Amendment. There are, however, two categories of domestic telephone numbers that were added to the NSA alert list [redacted] and the basis for their addition is slightly different.

~~(TS//SI//NF)~~ The first category consists of [redacted] domestic numbers that are currently the subject of FISC authorized electronic surveillance based on the FISC's finding of probable cause to believe that they are used by agents of [redacted] Since these numbers were already reviewed and authorized by the Court for electronic surveillance purposes, they were deemed approved for meta data querying without the approval of an NSA official.

~~(TS//SI//NF)~~ The second category consists of [redacted] domestic numbers each of which was added to the NSA alert list after coming to NSA's attention [redacted] and subsequent NSA analysis produced a sufficient level of suspicion that NSA generated an intelligence report about the telephone number to the FBI and the CIA [redacted]

~~(TS//SI//NF)~~ However, in order to avoid any appearance of circumventing the procedures, NSA will change its software to build the chains from the original foreign number and remove the [redacted] domestic numbers described above from the alert list. While the software is being developed, which will take approximately 45 days, NSA will continue to run the domestic numbers on the alert list as described.[1]

~~(TS//SI//NF)~~ As of the last day of the reporting period addressed herein, NSA had included a total of 3980 telephone numbers on the alert list, which includes foreign numbers and domestic numbers, after concluding that each of the foreign telephone numbers satisfied the standard set forth in the Court's May 24, 2006, and each of the domestic telephone numbers was either a FISC approved number or in direct contact with a foreign seed that met those criteria.

~~(TS//SI//NF)~~ To summarize the alert system: every day new contacts are automatically revealed with the 3980 telephone numbers contained on the alert list described above, which themselves are present on the alert list either because they satisfied the reasonable articulable suspicion standard, or because they are domestic numbers that were either a FISC approved number or in direct contact with a number that did so. These automated queries identify any new telephone contacts between the numbers on the alert list and any other number, except that domestic numbers do not alert on domestic-to-domestic contacts.

~~(TS//SI//NF)~~ During this reporting period, a combination of the alert system and queries resulting from leads described below in paragraph two led to analysis that resulted in the discovery of 138 new numbers that were tipped as leads to the FBI and the CIA as suspicious telephone numbers.

*See* Docket BR 06-05, NSA Report to the FISC, August 18, 2006, at 12-16 (footnote omitted). Subsequent NSA reports to the Court contained similar representations as to the functioning of the alert list process. *See, e.g.*, Docket BR 08-08, NSA 120-Day Report to the FISC, December 11, 2008, at 8-12.

~~(TS//SI//NF)~~ In short, the reports filed with the Court incorrectly stated that the telephone identifiers on the alert list satisfied the RAS standard. In fact, the majority of telephone identifiers included on the alert list had not been RAS approved, although the

[redacted]

identifiers were associated with the same class of terrorism targets covered by the Business Records Order.[2] Specifically, of the 17,835 telephone identifiers that were on the alert list on 15 January 2009 (the day DoJ reported this compliance incident to the Court), only 1,935 were RAS approved.[3]

**III. (U) NSA's Analysis:**

~~(TS//SI//NF)~~ [redacted] (The term "metadata" refers to information about a communication, such as routing information, date/time of the communication, *etc.*, but does not encompass the actual contents of a communication.) As explained in greater detail in Section VII of this declaration, analysis of communications metadata can yield important foreign intelligence information, [redacted]

[2] ~~(TS//SI//NF)~~ The initial BR FISA only covered [redacted]

[3] ~~(TS//SI//NF)~~ The reports filed with the Court in this matter also incorrectly stated the number of identifiers on the alert list. Each report included the number of telephone identifiers purportedly on the alert list. *See, e.g.*, Docket BR 06-08, NSA 120-Day Report to the FISC, August 18, 2006, at 15 ("As of the last day of the reporting period addressed herein, NSA has included a total of 3980 telephone numbers on the alert list . . . ."); Docket BR 08-13, NSA 120-Day Report to the FISC, December 11, 2008, at 11 ("As of November 2, 2008, the last day of the reporting period herein, NSA had included a total of 27,090 telephone identifiers on the alert list . . . ."). In fact, these numbers reported to the Court did not reflect the number of identifiers on the alert list; they actually represented the total number of identifiers included on the "station table" (discussed below at page15) as "RAS approved," *i.e.*, approved for contact chaining.

~~(TS//SI//NF)~~ [redacted], NSA put on the alert list telephone identifiers from two different sources that were of interest to counterterrorism personnel. The first source consisted of telephony identifiers against which the Agency was conducting SIGINT collection for counterterrorism reasons and the second source consisted of domestic telephony identifiers which, as a result of analytic tradecraft, were also deemed relevant to the Government's counterterrorism activity. The key goal of this alert process was to notify NSA analysts if there was a contact between a foreign telephone identifier of counterterrorism interest and any domestic telephone identifier; or contact between any domestic telephone identifier, related to a foreign counterterrorism target, and any foreign telephone identifier. At the time, NSA considered this type of contact to be an important potential piece of foreign intelligence since such contact could be indicative of an impending terrorist attack against the US homeland.[4]

**A. (TS) The Alert List Process**

~~(TS//SI//NF)~~ When the Court issued the first Business Records Order in May 2006, the [redacted] The first source was the "Address Database" which was a master target database of foreign and domestic telephone identifiers that were of current foreign intelligence interest to counterterrorism personnel.

[4] ~~(TS//SI//NF)~~ Neither the Agency nor the rest of the US Intelligence Community has changed this view regarding the importance of identifying this type of contact between counterterrorism targets and persons inside the United States. In fact, the 9/11 Commission Report alluded to the failure to share information regarding a facility associated with an al Qaeda safehouse in Yemen and contact with one of the 9/11 hijackers (al Mihdhar) in San Diego, California, as an important reason the Intelligence Community did not detect al Qaeda's planning for the 9/11 attack. *See*, "The 9/11 Commission Report," at 269-272.

The second source was [redacted] which was and continues to be a database NSA uses as a selection management system to manage and task identifiers for SIGINT collection.

~~(TS//SI//NF)~~ The Business Records Order states that "access to the archived data shall occur only when NSA has identified a known telephone identifier for which . . . there are facts giving rise to a reasonable articulable suspicion that the telephone identifier is associated with [redacted] Docket BR 08-13, Primary Order, 12 December 2008. The term "archived data" is of critical importance to understanding the rebuilt alert process NSA implemented after the Court issued the first Business Records Order in May 2006.

~~(TS//SI//NF)~~ As normally used by NSA in the context of the Agency's SIGINT activities, the term "archived data" refers to data stored in NSA's analytical repositories and excludes the many processing steps the Agency employs to make the raw collection useful to individual intelligence analysts.[5] Based on internal NSA correspondence and from discussions with NSA personnel familiar with the way NSA processes SIGINT collection, I have concluded this understanding of the term "archived data" meant that the NSA personnel who designed the BR FISA alert list process believed that the requirement to satisfy the RAS standard was only triggered when access was sought to NSA's stored (*i.e.*, "archived" in NSA parlance) repository of BR FISA data.

[5] ~~(TS//SI//NF)~~ For example, a small team of "data integrity analysts" ensures that the initial material NSA receives as a result of the Business Records Order is properly formatted and does not contain extraneous material that the Agency does not need or want before such material is made available to intelligence analysts.

~~(TS//SI//NF)~~ In fact, when the initial draft procedures for implementing the Business Records Order were created, it does not appear that either the SIGINT Directorate or the Office of General Counsel identified the use of non-RAS approved identifiers on the alert list as an issue that required in-depth analysis. NSA personnel, including the NSA attorney who reviewed the SIGINT Directorate's implementation procedures for the Business Records Order, appear to have viewed the alert system as merely pointing to a particular identifier on the alert list that required determination of *whether* the RAS standard had been satisfied before permitting contact chaining and/or pattern analysis in the archived BR FISA data. Accordingly, the Office of General Counsel approved the procedures but stressed that the RAS standard set out in the Business Records Order had to be satisfied before any access to the archived data could occur.[6]

~~(TS//SI//NF)~~ As a result, personnel in the SIGINT Directorate who understood how the automated alert process worked, based on their own understanding of the term "archived data" and the advice of NSA's Office of General Counsel, did not believe that NSA was required to limit the BR FISA alert list to only RAS approved telephone identifiers, [redacted]

[6] ~~(TS//SI//NF)~~ This result is not surprising since, regardless of whether the identifiers on the alert list were RAS approved, NSA was lawfully authorized to collect the conversations and metadata associated with the non-RAS approved identifiers tasked for NSA SIGINT collection activities under Executive Order 12333 and included on the alert list. The alert process was intended as a way for analysts to prioritize their work. The alerts did not provide analysts with permission to conduct contact chaining [redacted] of the BR FISA metadata. Instead, any contact chaining [redacted] of the BR FISA data also required a determination that the seed number for such chaining [redacted] had satisfied the RAS standard.

[redacted] Rather, they believed the limitation in the Court's order applied only where data had been aggregated over time, and where the authority and ability existed to conduct multi-hop analysis across the entire data archive. (See Section VII for a description of the benefits of aggregating data for later analysis.)

~~(TS//SI//NF)~~ NSA's review of this matter has confirmed that, even prior to the issuance of the Business Records Order, members of the SIGINT Directorate engaged in discussions with representatives of NSA's Office of General Counsel to determine how the Agency would process the telephony metadata NSA expected to receive pursuant to the Court's Order. Then, on 25 May 2006 immediately after issuance of the first Business Records Order, representatives of NSA's Signals Intelligence Directorate asked NSA's Office of General Counsel to concur on a draft set of procedures the SIGINT Directorate had developed to implement the Business Records Order. These draft procedures stated:

> The [redacted] ALERT processing system will provide a selective notification to the NSA CT AAD Shift Coordinator that a FISA Business Record transaction has been received. This notification will contain only the foreign telephone number and collection bin category. This notification will only occur when the foreign number in the transaction matches the foreign telephone number residing in that collection bin. This notification will include no domestic numbers and occurs prior to any chaining whatsoever.

There was no express statement that the alert list contained both RAS and non-RAS approved identifiers but it was clear that identifiers in the alert system would be

[redacted]

compared against incoming BR FISA data. It was also clear that, if there was a match between an identifier on the alert list and an identifier in the incoming data, a Shift Coordinator in the SIGINT Directorate's counterterrorism office would be notified.[8]

~~(TS//SI//NF)~~ Later on 25 May 2006, [redacted] of the Office of General Counsel concurred on the use of the draft procedures after adding language to the procedures emphasizing that analysts could not access the archived BR FISA data in NSA's BR FISA data repository unless the RAS standard had been satisfied. [redacted] coordinated her review of the procedures with one of her colleagues in the Office of General Counsel, [redacted] Specifically, as initially drafted, the procedures stated in pertinent part:

> The CT AAD Shift Coordinator will examine the foreign number and determine if that particular telephone number has been previously associated with [redacted] based on the standard articulated by the Court.

[redacted] revised this bullet to read:

> The CT AAD Shift Coordinator will examine the foreign number and determine if that particular telephone number has been previously associated with [redacted] based on the standard articulated by the Court. Reasonable articulable suspicion must be based on a totality of the circumstances and can be met by any number of factual scenarios. However, if a seed number is of interest only because of its direct contact with one other number, that other number must be known by some identifiable standard (probably or possibly) to be used by [redacted]. If you are unsure of whether the standard is met, please contact OGC.

[8] ~~(TS//SI//NF)~~ Since preparation of the original procedures, the Agency now refers to each "Shift Coordinator" as a "Homeland Mission Coordinator" or "HMC."

[redacted] also added a footnote to the procedures to read, "As articulated in the FISC Order, 'access to the archived data will occur only when the NSA has identified a known telephone number for which, based on the practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] Section 5A."

~~(TS//SI//NF)~~ The SIGINT Directorate began using the process described in the procedures not long after receiving OGC's approval. A copy of the procedures approved by NSA's Office of General Counsel and the approval of NSA's Office of General Counsel are attached as Exhibits A and B, respectively.

~~(TS//SI//NF)~~ As a result, the Agency ultimately designed the alert process to result in automated call chaining of the BR FISA data repository if the initial alert was based on a RAS approved identifier. If an alert was based on a non-RAS approved identifier, no automated chaining would occur in the BR FISA material but automated chaining could occur in NSA's repositories of information that had been acquired under circumstances where the RAS requirement did not apply, such as telephony collection that was not regulated by the FISA.

~~(TS//SI//NF)~~ Specifically, on 26 May 2006, [redacted] who was serving as the chief of NSA-Washington's counterterrorism organization in NSA's Signals Intelligence Directorate, directed that the alert list be rebuilt to ensure that the

alert list would only include identifiers assigned to "bins" or "zip codes"[9] that NSA used to label an identifier as being associated with [redacted] since these were the only classes of targets covered by the initial Business Records Order. Pursuant to this overall direction, personnel in the counterterrorism organization actually built two lists to manage the alert process. The first list – known as the alert list - included all identifiers that were of interest to counterterrorism analysts who were charged with tracking a [redacted] to include both foreign and domestic telephony identifiers. This list was used to compare the incoming telephony metadata NSA was obtaining from the Business Records Order and NSA's other sources of SIGINT collection to alert the counterterrorism organization if there was a match between a telephone identifier on the list and an identifier in the incoming metadata. This list had two partitions. The first partition consisted of RAS approved identifiers which could result in automated chaining of the BR FISA data repository. The second partition consisted of non-RAS approved identifiers which could not be used to initiate automated chaining of the archived BR FISA material. The second list – known as the "station table" - served as a historical listing of all telephone identifiers that have undergone a RAS determination, to include the results of the determination. This list was used to ensure that only RAS approved "seed" identifiers would be used to conduct chaining or pattern analysis of NSA's data repository for BR FISA material. For the Court's

[redacted]

convenience, a pictorial description of the BR FISA alert process as the process operated from May 2006 until January 2009 is attached as Exhibit C.

**B. ~~(TS)~~ Incorrect Description of Alert List in Reports to the FISC**

~~(TS//SI//NF)~~ Reviews of NSA records and discussions with relevant NSA personnel have revealed that [redacted] a managing attorney in NSA's Office of General Counsel, prepared the initial draft of the first BR FISA report. [redacted] appears to have included the inaccurate description of the BR FISA alert process due to a mistaken belief that the alert process for the Business Records Order

~~(TS//SI//NF)~~ After completing his initial draft of the BR FISA report, in an email prepared on Saturday, 12 August 2006, [redacted] wrote:

> Attached is the Draft of the Report to the Court. This is NOT ready to go until it is reviewed again... I have done my best to be complete and thorough, but ... make sure everything I have siad (*sic*) is absolutely true.

[redacted]

*See* Exhibit D. Despite the direction that the draft BR FISA report be thoroughly reviewed by other attorneys and NSA operational personnel for accuracy, the inaccurate description of the alert list that was contained in the initial draft of the report was not corrected before the report was finalized. In addition, the inaccurate description was not corrected in subsequent reports to the Court, either, until the inaccurate description was identified by representatives from the Department of Justice ("DoJ") during a briefing and roundtable discussion regarding NSA's handling of BR FISA material on 9 January 2009. Once DoJ confirmed that the Agency's actual alert list process in the BR FISA was inconsistent with the past descriptions NSA had provided to the Court of the alert list process, DoJ filed a notice on 15 January 2009 identifying this problem to the Court.

~~(TS//SI//NF)~~ As alluded to above, the inaccurate description of the BR FISA alert list initially appears to have occurred due to a mistaken belief that the alert list for the BR FISA material

This error was compounded by the fact that, as noted previously, the SIGINT Directorate had actually constructed the alert list with two partitions. Moreover, given that the Office of General Counsel prepared the initial draft of the report and had previously approved the procedures the SIGINT Directorate drafted for processing the BR FISA material, [redacted] as the primary reviewer of the draft report for the SIGINT Directorate, thought the Office of General Counsel's description of the automated alert process for BR FISA material, although omitting a discussion of one of the partitions, was legally correct since no contact chaining was

authorized to take place against the BR FISA archive unless the seed identifier for the chaining had undergone RAS approval.

~~(S//SI)~~ Therefore, it appears there was never a complete understanding among the key personnel who reviewed the report for the SIGINT Directorate and the Office of General Counsel regarding what each individual meant by the terminology used in the report. Once this initial misunderstanding occurred, the alert list description was never corrected since neither the SIGINT Directorate nor the Office of General Counsel realized there was a misunderstanding. As a result, NSA never revisited the description of the alert list that was included in the original report to the Court. Thus, the inaccurate description was also included in the subsequent reports to the Court.

~~(TS//SI//NF)~~ The initial Business Records Order was the subject of significant attention from NSA's Signals Intelligence Directorate, Office of General Counsel, and Office of Inspector General in an effort to ensure the Agency implemented the Order correctly. *See, e.g.,* NSA Office of Inspector General Report, "Assessment of Management Controls for Implementing the FISC Order: Telephony Business Records," dated 5 September 2006 (attached as Exhibit E).[11] Nevertheless, it appears clear in hindsight from discussions with the relevant personnel as well as reviews of NSA's internal records that the focus was almost always on whether analysts were contact chaining the Agency's repository of BR FISA data in compliance with the RAS standard

[11] ~~(TS//SI//NF)~~ Note that some of the Exhibits included with this declaration, such as Exhibit E, contain the control marking [redacted] or [redacted] NSA has de-compartmented these materials solely for the Court's consideration of the BR FISA compliance incident that DoJ reported to the Court on 15 January 2009.

specified in the Order. Similarly, subsequent internal NSA oversight of NSA's use of BR FISA material also appears to have focused on ensuring that:

- Homeland Mission Coordinators were applying the RAS standard correctly;
- Proper access control and labeling procedures were in place to ensure BR FISA material was controlled appropriately;
- The Agency was receiving and archiving the correct BR FISA telephony metadata;
- The Agency's dissemination of BR FISA reports containing US telephone identifiers were handled consistently with the terms of the Business Records Order and NSA reporting policies; and
- A process was put in place to conduct some auditing of the queries of the BR FISA *data repository*.

~~(TS//SI//NF)~~ Furthermore, from a technical standpoint, there was no single person who had a complete technical understanding of the BR FISA system architecture. This probably also contributed to the inaccurate description of the alert list that NSA included in its BR FISA reports to the Court.

## IV. (U) Corrective Actions:

### A. ~~(TS)~~ The Alert List

~~(TS//SI//NF)~~ Since DoJ reported this compliance matter to the Court on 15 January 2009, NSA has taken a number of corrective measures, to include immediate

steps to sequester, and shut off analyst access to, any alerts that were generated from comparing incoming BR FISA material against non-RAS approved identifiers. NSA also immediately began to re-engineer the entire alert process to ensure that material acquired pursuant to the Court's Business Records Order is only compared against identifiers that have been determined to satisfy the RAS standard since this was the description of the process that the Agency had provided to the Court. After an initial effort to fix the problem resulted in an unintended configuration of the revised automated alert process, NSA shut down the automated alert process entirely on 24 January 2009. (This configuration error resulted in DoJ filing a Supplemental Notice of Compliance Incident with the Court on 3 February 2009.) The automated alert process for BR FISA data will remain shut down until the Agency can ensure that all the intended changes to the automated BR FISA alert process will operate as intended and in a manner that match the descriptions NSA has provide to the Court. As appropriate, NSA plans to keep DoJ and the Court informed concerning the progress of this effort.

~~(TS//SI//NF)~~ In short, this redesign of the alert process will ensure that it is implemented in a manner that comports with the Court's Orders. NSA currently contemplates that there will actually be two, physically separate, alert lists. One list will consist solely of RAS approved identifiers and only this list will be used as a comparison point against the incoming BR FISA material. The second list will consist of a mix of RAS and non-RAS approved identifiers but will not be compared against the BR FISA data. In other words, BR FISA data will not be compared against non-RAS approved identifiers.

## B. (U) Other Measures Being Taken to Better Ensure Compliance With the Court's Orders

~~(TS//SI//NF)~~ In addition to the immediate measures the Agency took to address the compliance incident, I directed that the Agency complete ongoing end-to-end system engineering and process reviews (technical and operational) of NSA's handling of BR FISA material to ensure that the material is handled in strict compliance with the terms of the Business Records Order and the Agency's descriptions to the Court.[12] Detailed below are components of this end-to-end review and other steps being taken by NSA to ensure compliance with the Court's Orders.[13]

~~(TS//SI//NF)~~ For example, as part of the review that I have ordered, the Agency is examining the "Transaction Portal" analysts use to conduct one (1) hop chaining on RAS approved telephone identifiers for the purpose of validating network contacts, identified through previous, properly authorized contact chaining, for reporting on terrorist contacts with domestic telephone identifiers. The existing query mechanism for the Transaction Portal limits each query to a single "hop." In order that the results do not exceed the three (3) hop limit imposed by the Business Records Order the identifier entered by an analyst must either be RAS approved or must be within two (2) hops of the RAS approved identifier. Results from the query are returned to the analyst as a list of all individual call records associated with the identifier for the query. In theory, an analyst

[12] ~~(S)~~ NSA's SIGINT Director has directed similar reviews for some of the other sensitive activities NSA undertakes pursuant to its SIGINT authorities, to include certain activities that are regulated by the FISA, such as NSA's analysis of data received pursuant to the [redacted] If the Agency identifies any compliance issues related to activities undertaken pursuant to FISC authorization, NSA will bring such issues to the attention of DoJ and the Court.

[13] ~~(TS//SI//NF)~~ The results of this end-to-end review will be made available to DoJ and, upon request, to the FISC.

could conduct a series of one-hop queries to effectively conduct a multi-hop chain of the BR FISA data. The Agency is investigating whether software safeguards can be developed to enforce the three hop limit imposed by the Business Records Order.

~~(TS//SI//NF)~~ NSA initiated a review of the domestic identifiers on the "station table" that NSA uses as its historical record of RAS approval decisions on approved telephone identifiers so that NSA will be certain the Agency is in compliance with all aspects of the Business Records Order, to include the Agency's previous representations to the Court. As NSA's historical listing of all telephone identifiers that have undergone a RAS determination, the station table includes the results of each determination (*i.e.*, RAS approved or not RAS approved).

~~(TS//SI//NF)~~ Similar to the reviews of the Transaction Portal and the station table, NSA is examining other aspects of the Agency's technical architecture, to ensure that NSA's technical infrastructure has not allowed, and will not allow, non-approved selectors to be used as seeds for contact chaining of the BR FISA data. NSA will report to DoJ and the Court if this examination of the technical infrastructure reveals any incidents of improper querying of the BR FISA data repository.

~~(TS//SI//NF)~~ Although the Agency and DoJ have conducted previous audits of queries made against the BR FISA data, in response to the BR Compliance Order as well as in light of recent instances of improper querying that were the subject of separate notices to the Court, the Agency initiated an audit of all queries made of the BR FISA data repository since 1 November 2008 to determine if any of the queries during this

timeframe were made on the basis of non-RAS approved identifiers. While this review is still ongoing, to date this review has revealed no instances of improper querying of the BR FISA data repository, aside from improper queries made by two (2) analysts who were the subject of a previous compliance notice to the Court. From the time these two analysts were granted access to the BR FISA data repository on 11 and 12 December 2008 until the time NSA terminated their access in January 2009, these two analysts were responsible for 280 improper queries.

~~(TS//SI//NF)~~ Also, in response to some earlier instances of improper analyst queries of the BR FISA data repository that were recently discovered and reported to the Court, the Agency scheduled and delivered in-person briefings for all NSA personnel who have access to the BR FISA data archive to remind them of the requirements and their responsibilities regarding the proper handling of BR FISA material. NSA management personnel delivered these briefings with direct support from the Office of General Counsel and NSA's SIGINT Oversight & Compliance Office. In addition to the in-person briefings, all personnel with access to the BR FISA data archive have also received a written reminder of their responsibilities. As a follow-on effort, NSA's SIGINT Oversight & Compliance Office also initiated an effort to re-design the Agency's training for NSA operational personnel who require access to BR FISA material. The new training will include competency testing. If an analyst cannot achieve a passing grade on the test, he or she will not receive access to the BR FISA data repository.

~~(TS//SI//NF)~~ In an effort to eliminate the type of querying mistakes of the archived data that were the subject of other, separate compliance notices to the Court,

*see, e.g.*, DoJ Rule 10(c) Notices, filed 21 January 2009 and 26 January 2009, NSA is implementing changes to the system that analysts use to conduct contact chaining of the BR FISA repository so that the system will not be able to accept any non-RAS approved identifier as the seed identifier for call chaining analysis. Only a limited number of NSA personnel will possess privileges that would allow the new safety feature to be bypassed temporarily. NSA anticipates that the feature would only be bypassed for time sensitive queries where an NSA Homeland Mission Coordinator has determined that the seed identifier satisfies the RAS standard but operational priorities cannot wait for the formal update of the list of RAS approved identifiers to take effect within the system. Additionally, NSA is implementing software changes to the system that will limit the number of chained hops to only three from any BR FISA RAS approved selector.

**VI. (U) Answers to Court's Specific Questions:**

~~(TS//SI//NF)~~ ***Question 1****: Prior to January 15, 2009, who, within the Executive Branch, knew that the "alert list" that was being used to query the Business Record database included telephone identifiers that had not been individually reviewed and determined to meet the reasonable and articulable suspicion standard? Identify each such individual by name, title, and specify when each individual learned this fact.*

~~(TS//SI//NF)~~ Answer 1: As explained in the Agency's answer to Question 3, below, after DoJ identified this matter as a potential issue during DoJ's visit to NSA on 9 January 2009, numerous NSA and DoJ personnel were briefed about the problem. Accordingly, the identities of the some of the key personnel informed of the compliance

issue on or after 9 January 2009 are discussed in the answer to Question 3. The NSA personnel who, prior to 9 January 2009, knew, or may have known, that the alert list contained both RAS and non-RAS approved identifiers and were run against the incoming BR FISA data are as follows:

| Name | Title | Date of Knowledge | Distro for Reports |
|---|---|---|---|
| | Program Mgr CT Special Projects, SID | May 2006 | Yes |
| | Deputy Program Mgr, CT Special Projects, SID | May 2006 | Yes |
| | Deputy Program Mgr, CT Special Projects, A&P, SID | May 2006 | Yes |
| | NSA/OGC Attorney | May 2006 | Yes |
| | NSA/OGC Attorney | May 2006 | Yes |
| | [redacted] | May 2006 | No |
| | Computer Scientist SIGINT Dev'ment Strategy & Governance | May 2006 | No |
| | Tech Director HSAC, SID | May 2006 | No |
| | Deputy Chief HSAC, SID | January 2009 | No |
| | Computer Scientist HSAC, SID | May 2006 | No |
| | Tech Support | May 2006 | No |

Mission Systems
Mgmt, HSAC, SID

As ordered by the Court, the listing identifies the relevant personnel by their name, the title of the person's position with the Agency at the time they learned, or may have learned, that non-RAS identifiers were being run against the incoming BR FISA data, and the estimated date this information did or may have come to their attention. [redacted], whose name is denoted by an asterisk (*), has retired from Government service. Please note that the listing also indicates whether a person on the list was also on distribution for NSA's reports to the Court that contained the inaccurate description of the alert list. This does not mean that an individual who was on distribution for the reports was actually familiar with the contents of the reports.

~~(TS//SI//NF)~~ In addition to the individuals identified above, there were at least three (3) individuals [redacted] included as named addressees on her email concurrence to SIGINT Directorate's BR FISA implementation procedures on 25 May 2006. These individuals – [redacted] (NSA/OGC), [redacted] (NSA/OGC), and [redacted] (SID Data Acquisition) – are not included in the listing since they appear to have received the email for information purposes only and, based on conversations with each, do not appear to have been familiar with the implementation procedures that were attached to the email.

~~(TS//SI//NF)~~ It should also be noted there are an indeterminate number of other NSA personnel who knew or may have known the alert list contained both RAS and non-RAS selectors, but these personnel were not formally briefed on how the alert process

worked and were not responsible for its operation. Instead, they received alerts for the purpose of assessing RAS. Based on information available to me, I conclude it is unlikely that this category of personnel knew how the Agency had described the alert process to the Court.

~~(TS//SI//NF)~~ ***Question 2****: How long has the unauthorized querying been conducted?*

~~(TS//SI//NF)~~ **Answer 2**: The comparison of the incoming BR FISA material against the identifiers listed on the alert list began almost as soon as the first Business Records Order was issued by the Court on 24 May 2006.

~~*(TS//SI//NF)* ***Question 3***~~*: How did the unauthorized querying come to light? Fully describe the circumstances surrounding the revelations.*

~~(TS//SI//NF)~~ **Answer 3**: On 9 January 2009, representatives from the Department of Justice met with representatives from NSA in order to receive a briefing on NSA's handling of BR FISA material and then participated in a roundtable discussion of the BR FISA process.[14] During this briefing and follow-on discussion, DoJ representatives asked about the alert process. Upon receiving a description of the alert process from a representative of NSA's SIGINT Directorate, DoJ expressed concern that NSA may not have accurately described the alert list in its previous reports to the Court. After confirming its initial concern via an email response from NSA on 14 January 2009 to questions posed via email on 9 January 2009, DoJ filed a notice with the Court on

[14] ~~(TS//SI//NF)~~ NSA records indicate DoJ personnel attended at least eight BR FISA oversight sessions prior to the session on 9 January 2009 when the error was discovered but there is no indication that the use of non-RAS approved identifiers on the alert list was ever raised or discussed at these prior sessions.

15 January 2009 regarding this compliance matter. The following individuals participated in the briefing and discussion on 9 January 2009:

**NSA Attendees**

[redacted]

**DoJ Attendees**

(S) I understand that DoJ informed the FBI's Office of General Counsel of this compliance incident on 23 January 2009. In addition, on 30 January 2009, I personally mentioned to the new Director of National Intelligence ("DNI"), Dennis Blair, that NSA was investigating this compliance matter. The DNI received additional information about the compliance incident on 4 February 2009, from the DNI General Counsel, Benjamin Powell, and on 12 February 2009 I provided further information to the DNI regarding the incident. Internally, NSA notified its Inspector General of this compliance matter sometime after DoJ notified the Court on 15 January 2009. In accordance with Department of Defense requirements, NSA is in the process of formally reporting this compliance matter to the Assistant Secretary of Defense for Intelligence Oversight as part of NSA's current Quarterly Intelligence Oversight Report. In the manner specified by Department of Defense and DNI regulations, the Quarterly Report will also be provided to the President's Intelligence Oversight Board ("IOB"). I expect the notification to the

IOB will occur, concurrent with, or shortly after the filing of this declaration with the Court. In addition to preparing the formal notification required by the Defense Department's procedures, on 10 February 2009 I provided detailed information about this compliance matter to the Undersecretary of Defense for Intelligence, James Clapper.

~~(TS//SI//NF)~~ ***~~Question 4~~:*** *The application signed by the Director of the Federal Bureau of Investigation, the Deputy Assistant Attorney General for National Security, United States Department of Justice ("DOJ"), and the Deputy Attorney General of the United States as well as the declaration of* [redacted] *a Deputy Program Manager at the National Security Agency ("NSA"), represents that during the pendency of this order, the NSA Inspector General, the NSA General Counsel, and the NSA Signals Intelligence Directorate Oversight and Compliance Office each will conduct reviews of this program. Docket BR 08-13, Application at 27, Declaration at 11. The Court's Order directed such review. Id., Primary Order at 12. Why did none of these entities that were ordered to conduct oversight over this program identify the problem earlier? Fully describe the manner in which each entity has exercised its oversight responsibilities pursuant to the Primary Order in this docket as well as pursuant to similar predecessor Orders authorizing the bulk production of telephone metadata.*

~~(TS//SI//NF)~~ **~~Answer 4~~**: As described earlier in this declaration, the oversight activities of NSA's Office of General Counsel, Office of Inspector General, and SIGINT Directorate Oversight & Compliance Office generally focused on how RAS determinations were made; the ingestion of BR FISA data; and ultimately on the querying of BR FISA data once it had been stored in the data repository NSA maintains

for BR FISA data. From May 2006 until January 2008, there were monthly, in-person "due diligence" meetings of oversight and operational personnel to monitor NSA's implementation of a number of sensitive NSA SIGINT activities, to include NSA's activities under the Business Records Order.[15] Although each office exercised regular oversight of the program, the initial error in the description of the alert list was not caught by either the Office of General Counsel nor the SIGINT Directorate's Oversight & Compliance Office.

~~(TS//SI//NF)~~ Agency records indicate that, in April 2006, when the Business Records Order was being proposed, NSA's Office of Inspector General ("OIG") suggested to SID personnel that the alert process be spelled out in any prospective Order for clarity but this suggestion was not adopted. Later in 2006 when OIG conducted a study regarding the adequacy of the management controls NSA adopted for handling BR FISA material, OIG focused on queries of the archived data since the SIGINT Directorate had indicated to OIG through internal correspondence that the telephone identifiers on the alert list were RAS approved. OIG's interest in the alert list came from OIG's understanding that the alert list was used to cue automatic queries of the specific analytic database where the BR FISA material was stored by the Agency. At least one employee of the SIGINT Directorate thought that OIG had been briefed about how the alert process worked. Regardless of the accuracy of this employee's recollection, like other NSA offices OIG also believed that the "archived data" referred to in the order was the analytic repository where NSA stored the BR FISA material.

[15] ~~(S//SI)~~ The Agency canceled the due diligence meetings in January 2008 since NSA management determined that monthly, in-person meetings were no longer necessary.

~~(TS//SI//NF)~~ OIG continued to monitor NSA's implementation of the Business Records Order throughout the relevant timeframe (2006-2009) by reviewing specific BR FISA compliance incidents; following up with the relevant NSA organization regarding the status of recommendations OIG made in a Special Study report on the BR FISA dated 5 September 2006; and attending the due diligence meetings NSA held until January 2008 regarding the status of a number of sensitive NSA SIGINT activities, to include the BR FISA activity. With respect to OIG's monitoring of the SIGINT Directorate's progress in implementing recommendations from OIG's September 2006 Special Study, OIG asked for and evaluated the SIGINT Directorate's progress responding to OIG's recommendations.

~~(TS//SI//NF)~~ Since the issuance of the first Business Records Order in May 2006, the BR FISA activity has received oversight attention from all three NSA organizations charged by the Court with conducting oversight. For example, in addition to OIG's oversight activities mentioned above, beginning in August 2008 the SIGINT Directorate, with support from the Office of General Counsel, has conducted regular spot checks of analyst queries of the BR FISA data repository. The Office of General Counsel has also had regular interaction with SIGINT and oversight personnel involved in BR FISA issues in order to provide legal advice concerning access to BR FISA data. The Office of General Counsel has also conducted training for personnel who require access to BR FISA material; participated in due diligence meetings; and prepared materials for the renewal of the Business Records Order. All of these activities allowed the Office of General Counsel to monitor the Agency's implementation of the Business Records Order.

~~(TS//SI//NF)~~ As a further illustration of the attention the Agency paid to the BR FISA Order, attached to this declaration are, respectively, copies of the Court-ordered review of NSA's BR FISA implementation, dated 10 July 2006, which was conducted jointly by OIG and the Office of General Counsel (Exhibit F); the SIGINT Oversight & Compliance Office's BR FISA Audit Plan from 11 July 2006 (Exhibit G); OIG's September 2006 Special Study of the BR FISA(previously identified as Exhibit E); and the implementation procedures for the Business Records Order that were reviewed and approved by NSA's Office of General Counsel (previously identified as Exhibit B).

~~(TS//SI//NF) In~~ addition, it is important to note that NSA personnel were always forthcoming with internal and external personnel, such as those from the Department of Justice, who conducted oversight of the Agency's activities under the Business Records Order. I have found no indications that any personnel who were knowledgeable of how NSA processed BR FISA material ever tried to withhold information from oversight personnel or that they ever deliberately provided inaccurate information to the Court.

~~(TS//SI//NF)~~ ***Question 5****: The preliminary notice from DOJ states that the alert list includes telephone identifiers that have been tasked for collection in accordance with NSA's SIGINT authority. What standard is applied for tasking telephone identifiers under NSA's SIGINT authority? Does NSA, pursuant to its SIGINT authority, task telephone identifiers associated with United States persons? If so, does NSA limit such identifiers to those that were not selected solely upon the basis of First Amendment protected activities?*

~~(TS//SI//NF)~~ ~~Answer 5~~: *SIGINT Tasking Standard*: Although the alert list included telephone identifiers of counterterrorism targets that had not been assessed against the RAS standard or had been affirmatively determined by NSA personnel not to meet the RAS standard, such identifiers were not tasked in a vacuum. Whether or not an identifier is assessed against the RAS standard, NSA personnel may not task an identifier for any sort of collection or analytic activity pursuant to NSA's general SIGINT authorities under Executive Order 12333 unless, in their professional analytical judgment, the proposed collection or analytic activity involving the identifier is likely to produce information of foreign intelligence value. In addition, NSA's counterterrorism organization conducted reviews of the alert list two (2) times per year to ensure that the categories (zip codes) used to identify whether telephone identifiers on the alert list remained associated with [redacted] or one of the other target sets covered by the Business Records Order. Also, on occasion the SIGINT Directorate changed an identifier's status from RAS approved to non-RAS approved on the basis of new information available to the Agency.

(U) *US Person Tasking*: NSA possesses some authority to task telephone identifiers associated with US persons for SIGINT collection. For example, with the US person's consent, NSA may collect foreign communications to, from, or about the US person. In most cases, however, NSA's authority to task a telephone number associated with a US person is regulated by the FISA. For the Court's convenience, a more detailed description of the Agency's SIGINT authorities follows, particularly with respect to the collection and dissemination of information to, from, or about US persons.

~~(TS//SI//NF)~~ NSA's general SIGINT authorities are provided by Executive Order 12333, as amended (to include the predecessors to the current Executive Order); National Security Council Intelligence Directive No. 6; Department of Defense Directive 5100.20; and other policy direction. In particular, Section 1.7(c) of Executive Order 12333 specifically authorizes NSA to "Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign intelligence and counterintelligence purposes to support national and departmental missions." However, when executing its SIGINT mission, NSA is only authorized to collect, retain or disseminate information concerning United States persons in accordance with procedures approved by the Attorney General.[16] The current Attorney General approved procedures that NSA follows are contained in Department of Defense Regulation 5240.1-R, and a classified annex to the regulation governing NSA's electronic surveillance activities.

(U) Moreover, some, but not all, of NSA's SIGINT activities are also regulated by the Foreign Intelligence Surveillance Act. For example, since the amendment of the FISA in the summer of 2008, if NSA wishes to direct SIGINT activities against a US person located outside the United States, any SIGINT collection activity against the US person generally would require issuance of an order by the FISC. For SIGINT activities executed pursuant to an order of the FISC, NSA is required to comply with the terms of

[16](U) The FISA and Executive Order 12333 both contain definitions of the term "United States person" which generally include a citizen of the United States; a permanent resident alien; an unincorporated association substantially composed of US citizens or permanent resident aliens; or a corporation that is incorporated in the US, except for a corporation directed and controlled by a foreign government(s).

the order and Court-approved minimization procedures that satisfy the requirements of 50 U.S.C. § 1801(h).

(U) *First Amendment Considerations*: For the following reasons, targeting a US person solely on the basis of protected First Amendment activities would be inconsistent with restrictions applicable to NSA's SIGINT activities. As part of their annual intelligence oversight training, NSA personnel are required to re-familiarize themselves with these restrictions, particularly the provisions that govern and restrict NSA's handling of information of or concerning US persons. Irrespective of whether specific SIGINT activities are undertaken under the general SIGINT authority provided to NSA by Executive Order 12333 or whether such activity is also regulated by the FISA, NSA, like other elements of the US Intelligence Community, must conduct its activities "with full consideration of the rights of United States persons." *See* Section 1.1(a) of Executive Order 12333, as amended. The Executive Order further provides that US intelligence elements must "protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law." *Id.* at Section 1.1(b).

(U) Consistent with the Executive Order's requirement that each intelligence agency develop Attorney General approved procedures that "protect constitutional and other legal rights" (EO 12333 at Section 2.4), DoD Regulation 5240.1-R prohibits DoD intelligence components, including NSA, from collecting or disseminating information concerning US persons' "domestic activities" which are defined as "activities that take place in the domestic United States that do not involve a significant connection to a

foreign power, organization, or person." *See, e.g.,* Section C2.2.3 of DoD Regulation 5240.1-R. In light of this language, targeting a US person solely on the basis of protected First Amendment activities would be inappropriate.

~~(TS//SI//NF)~~ ***Question 6:*** *In what form does the government retain and disseminate information derived from queries run against the business records data archive?*

~~(TS//SI//NF)~~ **Answer 6**: Through 29 July 2008, NSA archived the reports the Agency disseminated from its analysis of data in the BR FISA data repository in a special program-specific limited access data repository [redacted] as well as on a restricted access group of Lotus Notes servers. Reporting was transitioned to traditional NSA "I-Series" format on 29 July 2008. I-Series reports are retained in NSA's limited access sensitive reporting data repository [redacted] Copies of the I-Series reports are also kept in [redacted] to allow them to be searched with special software tools. In addition, the I-Series reports are stored on ESECS, the Extended Enterprise Corporate Server. Access to these reports in ESECS is appropriately restricted. As directed by the Business Records Order, information in the BR FISA data archive is retained five (5) years.

~~(TS//SI//NF)~~ In response to Question 6, the Agency has also conducted a review of all 275 reports of domestic contacts NSA has disseminated as a result of contact chaining [redacted] of the NSA's archive of BR FISA material.[17] NSA has

[17] ~~(TS//SI//NF)~~ Note that a single report may tip more than one telephone identifier as being related to the seed identifier. As a result, the 275 reports have tipped a total of 2,549 telephone identifiers since 24 May 2006. Also note that, of the 275 reports that were disseminated, 31 resulted from the automated alert process.

identified no report that resulted from the use of a non-RAS approved identifier as the initial seed identifier for chaining through the BR FISA material.[18] Of the 275 reports that were generated, 22 reports were based on a US identifier serving as the initial seed identifier. For each of these reports, the initial US seed identifier was either already the subject of FISC-approved surveillance based on the FISC's finding of probable cause to believe that they are used by agents of [redacted] or the initial US seed identifier had been reviewed by NSA's Office of General Counsel as part of a RAS determination to ensure that the RAS determination was not based solely on a US person's protected First Amendment activities. Almost invariably, the RAS determinations that the Office of General Counsel reviewed were based on direct contact between the telephone identifier and another identifier already known to be associated with one of the terrorist organizations or entities listed in the Business Records Order.

~~(TS//SI//NF)~~ For the Court's convenience, a copy of the type of report that NSA was issuing prior to 9 January 2009 is attached to this declaration as Exhibit H so the Court can see how the material was reported and to whom. Also attached as Exhibit I is an example of an alert generated by the automated alert system, prior to the Agency's decision on 23 January 2009 to shut down the BR FISA alerts. (The decision was actually effected in the early morning hours of 24 January 2009).

[18] ~~(TS//SI//NF)~~ The Agency has identified one (1) report where the number on the alert list was not RAS approved when the alert was generated but, after receiving the alert, a Homeland Mission Coordinator determined that the identifier, in fact, satisfied the RAS standard. After this determination, the Agency subsequently used the identifier as a seed for chaining in the BR FISA data archive. Ultimately, information was developed that led to a report to the FBI that tipped 11 new telephone identifiers.

~~(TS//SI//NF)~~ Unlike reports, which NSA disseminated outside NSA, the alerts were only disseminated inside NSA to SIGINT personnel responsible for counterterrorism activity. Initially, if an identifier on the alert list generated an alert that the identifier had been in contact with an identifier in the United States, the alert system masked (*i.e.*, concealed) the domestic identifier. Later, in January 2008, the SIGINT Directorate allowed the alerts to be sent to analysts without masking the domestic identifier. NSA made this change in an effort to improve the ability of SIGINT analysts, on the basis of their target knowledge, to prioritize their work more efficiently.

~~(TS//SI//NF)~~ ***Question 7****: If ordered to do so, how would the government identify and purge information derived from queries run against the business records data archive using telephone identifiers that were not assessed in advance to meet the reasonable and articulable suspicion standard?*

(TS//~~SI~~//NF) **Answer 7**: NSA has not authorized its personnel to use non-RAS approved identifiers to conduct chaining or pattern analysis of NSA's analytic repository of BR FISA material. On those occasions where improper querying of this data archive has been discovered, the Agency has taken steps to purge data and correct whatever deficiencies that led to the querying mistakes.

(TS//~~SI~~//NF) With respect to the alert process, after this compliance matter surfaced, NSA identified and eliminated analyst access to all alerts that were generated from the comparison of non-RAS approved identifiers against the incoming BR FISA material. The only individuals who retain continued access to this class of alerts are the

Technical Director for NSA's Homeland Security Analysis Center ("HSAC") and two system developers assigned to HSAC. From a technical standpoint, NSA believes it could purge copies of any alerts that were generated from comparisons of the incoming BR FISA information against non-RAS approved identifiers on the alert list. However, the Agency, in consultation with DoJ, would need to determine whether such action would conflict with a data preservation Order the Agency has received in an ongoing litigation matter.

**VII. (~~TS//SI//NF~~) Value of the BR FISA Metadata**

(~~TS//SI//NF~~) As discussed in prior declarations in this matter, including my declaration in docket number BR 06-05, access to the telephony metadata collected in this matter is vital to NSA's counterterrorism intelligence mission. It is not possible to target collection solely on known terrorist telephone identifiers and at the same time use the advantages of metadata analysis to discover the enemy because operatives of [redacted] (collectively, the "Foreign Powers") take affirmative and intentional steps to disguise and obscure their communications and their identities. They do this using a variety of tactics, including, regularly changing telephone numbers, [redacted] The only effective means by which NSA analysts are able continuously to keep track of the Foreign Powers, and all operatives of the Foreign

Powers making use of such tactics, is to obtain and maintain telephony metadata that will permit these tactics to be uncovered.

~~(TS//SI//NF)~~ Because it is impossible to determine in advance which particular piece of metadata will turn out to identify a terrorist, collecting metadata is vital for success. To be able to exploit metadata fully, the data must be collected in bulk. Analysts know that the terrorists' telephone calls are located somewhere in the billions of data bits; what they cannot know ahead of time is exactly where. The ability to accumulate metadata substantially increases NSA's ability to detect and identify members of the Foreign Powers. Specifically, the NSA performs queries on the metadata: contact-chaining [redacted]

~~(TS//SI//NF)~~ When the NSA performs a contact-chaining query on a terrorist-associated telephone identifier computer algorithms will identify all the contacts made by that identifier and will automatically identify the further contacts made by that first tier of contacts. In addition, the same process is used to identify a third tier of contacts, which includes all identifiers in contact with the second tier of contacts. The collected metadata thus holds contact information that can be immediately accessed as new terrorist-associated telephone identifiers are identified. Multi-tiered contact analysis is useful for telephony, because unlike e-mail, which involves the heavy use of spam, a telephonic device does not lend itself to simultaneous contact with large numbers of individuals.

~~(TS//SI//NF)~~ One advantage of the metadata collected in this matter is that it is historical in nature, reflecting contact activity from the past that cannot be captured in the present or prospectively. In addition, metadata may also be very timely and well suited for alerting against suspect activity. To the extent that historical connections are

important to understanding a newly-identified target, metadata may contain links that are absolutely unique, pointing to potential targets that otherwise would be missed. [redacted]

[redacted]

Other advantages of contact chaining include [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

[redacted]

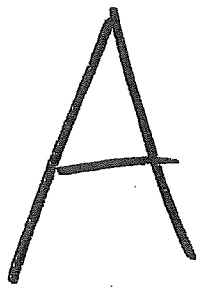
~~(TS//SI//NF)~~ The foregoing discussion is not hypothetical. As noted previously, since inception of the first Business Records Order, NSA has provided 275 reports to the FBI. These reports have tipped a total of 2,549 telephone identifiers as being in contact with identifiers associated with [redacted] and affiliated terrorist organizations. Upon receipt of the reporting from NSA, the FBI has sent investigative leads to relevant FBI Field Offices for investigative action. FBI representatives have indicated to NSA as recently as 9 February 2009 that the telephone contact reporting has provided leads and linkages to individuals in the U.S. with potential terrorism ties who may not have otherwise been known to or identified by the FBI. For example, attached as Exhibit J is feedback from the FBI on the report that NSA has included as Exhibit H.

(U) I declare under penalty of perjury that the facts set forth above are true and correct.

VR

KEITH B. ALEXANDER
Lieutenant General, U.S. Army
Director, National Security Agency

Executed this 13TH day of February, 2009



**From:** [redacted] (CIV-NSA) D21
**Sent:** Thursday, May 25, 2006 6:07 PM
**To:** [redacted] (CIV-NSA) S2I5; [redacted] (CIV-NSA)D21; [redacted] (CIV-NSA) D21; DL AADSC
**Cc:** [redacted] (CIV-NSA) [redacted] (CIV-NSA) [redacted]; [redacted] (CIV-NSA) [redacted] (CIV-NSA) D21; [redacted] (CIV-NSA) D21
**Subject:** (U) OGC Changes to RE: (U) Proposed Interim Procedures.

**Classification:** ~~TOP SECRET//COMINT//NOFORN//MR~~

Shift Supervisors,

OGC has added clarification language to the procedures [redacted] sent earlier today. Please use the modified document.

[redacted]

If you would like to discuss further tomorrow, please contact [redacted] (I'm on leave).

[redacted]

[redacted]
Attorney
Office of General Counsel
963-3121(s)/[redacted]
Ops2B, 2B8134, Suite 6250

-----Original Message-----
**From:** [redacted] (CIV-NSA) S2I5
**Sent:** Thursday, May 25, 2006 2:13 PM
**To:** [redacted] (CIV-NSA) D21; [redacted] (CIV-NSA)D21; [redacted] (CIV-NSA) D21
**Cc:** [redacted] (CIV-NSA) [redacted] (CIV-NSA) [redacted]; [redacted] (CIV-NSA) S
**Subject:** (U) Proposed Interim Procedures.

**Classification:** ~~TOP SECRET//COMINT//NOFORN//MR~~

OGC, please review and provide comments.

Thanks,

[redacted]
<<...>>

[redacted]
Counter Terrorism Primary Production Center
963-0491, Room 2B3116
[redacted]
[redacted]
Suite 6276

Classification: ~~TOP SECRET//COMINT//NOFORN//MR~~

B

~~(C)~~ Interim procedures to ensure CT AAD is in compliance with FISC Business Records Order:

1. ~~(TS//SI//NF)~~ All foreign telephone numbers analyzed against the FISA Business Records acquired under Docket Number: BR 06-05 approved on 24 May 2006 will adhere to the following:
   - The [redacted] ALERT processing system will provide a selective notification to the NSA CT AAD Shift Coordinator that a FISA Business Record transaction has been received. This notification will contain only the foreign telephone number and collection bin category. This notification will only occur when the foreign number in the transaction matches the foreign telephone number residing in that collection bin. This notification will include no domestic numbers and occurs prior to any chaining whatsoever.
   - The CT AAD Shift Coordinator will examine the foreign number and determine if that particular telephone number has been previously associated with [redacted] based on the standard articulated by the Court[1]. Reasonable articulable suspicion must be based on a totality of the circumstances and can be met by any number of factual scenarios. However, if a seed number is of interest only because of its direct contact with one other number, that other number must be known by some identifiable standard (probably or possibly) to be used by [redacted] organization. If you are unsure of whether the standard is met, please contact OGC.
   - Once the CT AAD Shift Coordinator has made a positive determination the number will be processed for chaining [redacted] against the FISA Business Records acquire under Docket Number: BR 06-05.

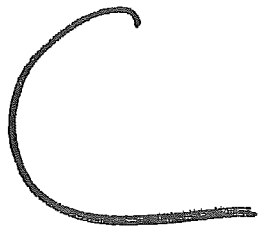
2. ~~(TS//SI//NF)~~ All domestic and most foreign collection bins which had been processing [redacted] have been suspended. The exception is active FISC FISA approved telephone numbers.
3. ~~(TS//SI//NF)~~ CT AAD will rebuild these collection bins starting with the selective notifications sent to the NSA CT AAD Shift Coordinator that a FISA Business Record transaction has been received. (as describe above)
4. The CT AAD Shift must independently review each number gleaned from all published reports. For example NSA and CIA reporting

[1] As articulated in the FISC Order, "access to the archived data will occur only when the NSA has identified a known telephone number for which, based on the practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] Section 5A.

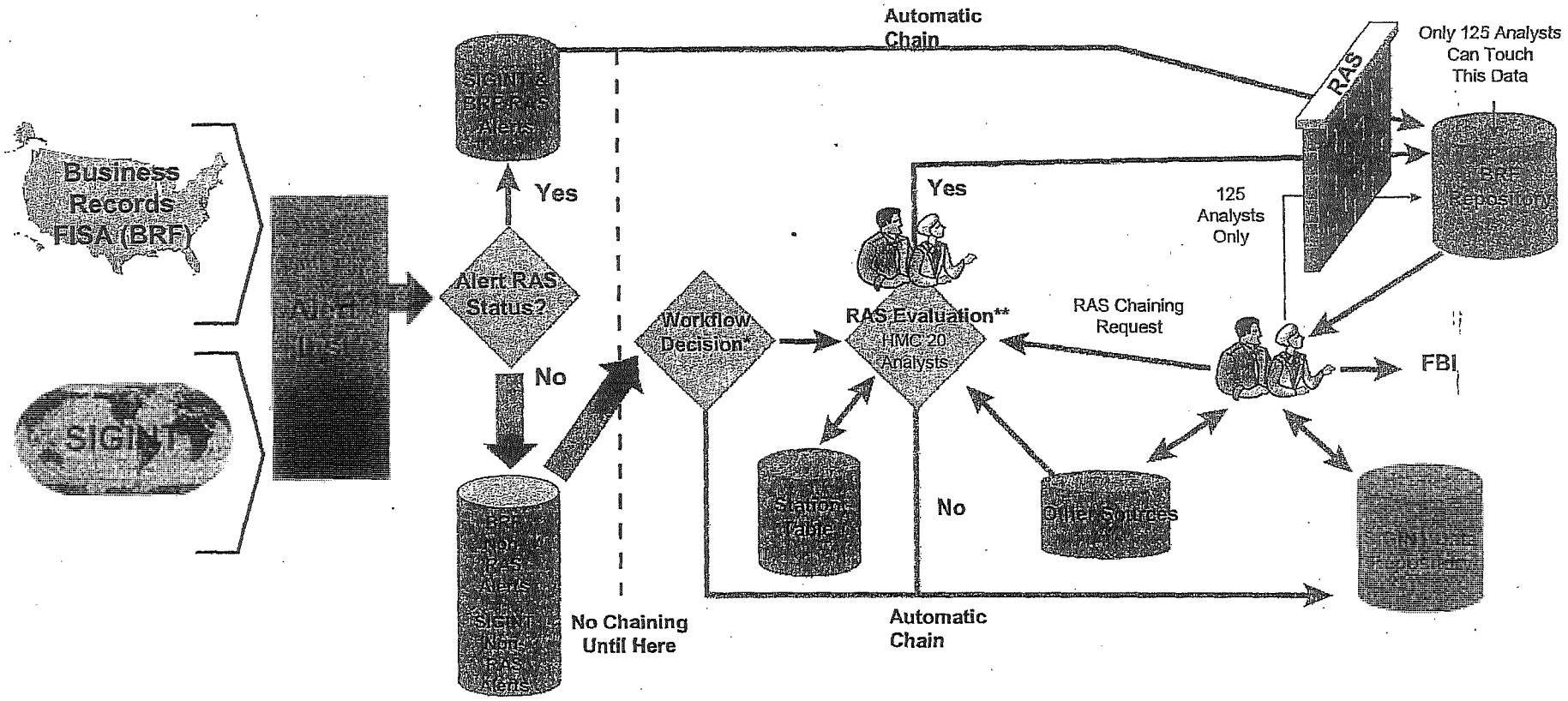
Derived From: NSA/CSSM 1-52
~~Dated: 20070108~~
Declassify On: 20310403

5. ~~(TS//SI//NF)~~ Simultaneously, the CT AAD will conduct a review of the approximate 12,000 [redacted] number which currently resided in these bins
6. ~~(TS//SI//NF)~~ These interim steps will allow all alerting processes to continue with the added measure necessary to comply with FISA Business Record order, Docket Number: BR 06-05.

FN 1: ~~(TS//SI//NF)~~ As articulated in the FISC Order, "access to the archived data shall occur only when NSA has identified a known telephone number for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted]" (BR Order, Docket BR 06-05, Section 5(A)).



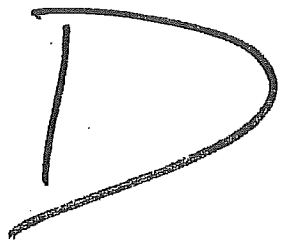
# Former Process (May 06 – Jan 09)




* Workflow decision based on available Homeland Mission Coordinators (HMC) and volume of alerts.

** RAS decision by HMC, who evaluates all available intelligence and open source data to determine if the combined information indicates the suspect phone selector is a terrorist selector as defined by the Court.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108



**From:** [redacted](CIV-NSA)D21
**Sent:** Saturday, August 12, 2006 12:03 PM
**To:** [redacted](CIV-NSA) D21; [redacted](CIV-NSA) [redacted] CIV-NSA) S2; [redacted](CIV-NSA)D21; [redacted] (CIV-NSA)D21
**Cc:** [redacted](CIV-NSA) D21; [redacted](CIV-NSA) D21; [redacted] (CIV-NSA) D21
**Subject:** (U) Report to Court on Business Record Activity
**Importance:** High

**Classification:** ~~TOP SECRET//COMINT//ORCON/NOFORN//20291123~~

Hi all-

Here is where we stand on the metadata [redacted]

[redacted] expire on Friday.

All of the draft docs are in the shared directory, under OPSPROGRAM FISA/BUSINESS RECORDS/BR FISA AUG 06 RENEWAL, except there is a separate folder entitled REPORTS TO COURT in wich the BR report is located.

We have sent to DoJ draft copies of the application for renewal, the declaraton (which [redacted]'s going to complete, rather than the DIRNSA (unless DoJ squawks)), and the Orders. We should hear from them early in the week about any needed revisions, and they want to provide to the judge on Thursday am. I am hoping [redacted] can be in charge of changes to it, and [redacted] can supervise and/or assist her.

Attached is the Draft of the Report to the Court. This is NOT ready to go until it is reviewed again by [redacted] I have done my best to be complete and thorough, but [redacted] needs to make sure everything I have siad is absolutely true, and you guys need to make sure it makes sense and will satisfy the Court. You MUST feel free to edit as you think appropriate; dont stick to what I have said if there is a better way to say it.

Someone needs to format the thing too, make sure spacing, numbering, etc are all good [redacted] and we need to get this into DOJ's hands as quickly as we are able.

[redacted]

Thanks for all your help and have a great week. [redacted]

[redacted]
Associate General Counsel
(Operations)
963-3121

~~Derived From: NSA/CSSM 1-52~~

~~Dated: 20041123~~

~~Declassify On: 20291123~~

~~Classification: TOP SECRET//COMINT//ORCON/NOFORN//20291123~~

E

# National Security Agency/Central Security Service

Further dissemination of this report outside the Office of the Inspector General, NSA is *PROHIBITED* without the approval of the Inspector General.


# Inspector General Report

## ~~(TS//SI//NF)~~ REPORT ON THE ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDER: TELEPHONY BUSINESS RECORDS

ST-06-0018
5 SEPTEMBER 2006

~~DERIVED FROM: NSA/CSSM 1-52~~
~~DATED: 20041123~~
~~DECLASSIFY ON: MR~~

## (U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the Director, NSA/Chief, CSS, the Office of the Inspector General (OIG) conducts inspections, audits, and investigations. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA/CSS operations; to provide intelligence oversight; to protect against fraud, waste, and mismanagement of resources; and to ensure that NSA/CSS activities are conducted in compliance with the Constitution, laws, executive orders, regulations, and directives. The OIG also serves as ombudsman, assisting all NSA/CSS employees and affiliates, civilian and military.

## (U) INSPECTIONS

(U) The inspection function conducts management and program evaluations in the form of organizational and functional reviews, undertaken either as part of the OIG's annual plan or by management request. The inspection team's findings are designed to yield accurate and up-to-date information on the effectiveness and efficiency of entities and programs, along with an assessment of compliance with laws and regulations; the recommendations for corrections or improvements are subject to followup. The inspection office also partners with the Inspectors General of the Service Cryptologic Elements to conduct joint inspections of the consolidated cryptologic facilities.

## (U) AUDITS

(U) The internal audit function is designed to provide an independent assessment of programs and organizations. Performance audits evaluate the economy and efficiency of an entity or program, as well as whether program objectives are being met and operations are in compliance with regulations. Financial audits determine the accuracy of an entity's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

## (U) INVESTIGATIONS AND SPECIAL INQUIRIES

(U) The OIG administers a system for receiving and acting upon requests for assistance or complaints (including anonymous tips) about fraud, waste and mismanagement. Investigations and Special Inquiries may be undertaken as a result of such requests or complaints; at the request of management; as the result of irregularities that surface during an inspection or audit; or at the initiative of the Inspector General.

OFFICE OF THE INSPECTOR GENERAL
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

5 September 2006
IG-10693-06

TO: DISTRIBUTION

SUBJECT: ~~(TS//SI//NF)~~ Report on the Assessment of Management Controls for Implementing the Foreign Intelligence Surveillance Court (FISC) Order: Telephony Business Records (ST-06-0018)—ACTION MEMORANDUM

1. ~~(TS//SI//NF)~~ This report summarizes the results of our assessment of Management Controls for Implementing the FISC Order: Telephony Business Records. The report incorporates management's response to the draft report.

2. ~~(U//FOUO)~~ As required by NSA/CSS Policy 1-60, *NSA/CSS Office of the Inspector General*, actions on OIG audit recommendations are subject to monitoring and followup until completion. Consequently, we ask that you provide a written status report concerning each planned corrective action categorized as "OPEN." The status report should provide sufficient information to show that corrective actions have been completed. If a planned action will not be completed by the original target completion date, please state the reason for the delay and give a revised target completion date. Status reports should be sent to [redacted] Assistant Inspector General, at OPS 2B, Suite 6247, within 15 calendar days after each target completion date.

3. ~~(U//FOUO)~~ We appreciate the courtesy and cooperation extended to the auditors throughout the review. If you need clarification or additional information, please contact [redacted] Assistant Inspector General, on 963-2988 or via e-mail at [redacted]

Brian R. McAndrew
BRIAN R. MCANDREW
Acting Inspector General

Derived From: NSA/CSSM 1-52
Dated: 20041123
Declassify On: MR

DISTRIBUTION:
DIR
D/DIR
SIGINT Director
SID Program Manager for CT Special Projects, S
Chief, SID O&C
SSG1, [redacted]
SID Deputy Director for Customer Relationships
SID Deputy Director for Analysis and Production
Chief, S2I5
SID Deputy Director for Data Acquisition
Chief, S332
GC
AGC(O)

# ~~(TS//SI//NF)~~ ASSESSMENT OF MANAGEMENT CONTROLS FOR IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC) ORDER: TELEPHONY BUSINESS RECORDS

~~(TS//SI//[redacted]//OC,NF)~~ **Background:** The Order of the FISC issued 24 May 2006 in *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from* [Telecommunications Providers] *Relating to* [redacted] *in the United States and Abroad*, No. BR-06-05 (the Order) states that "[t]he Inspector General and the General Counsel shall submit a report to the Director of NSA (DIRNSA) 45 days after the initiation of activity [permitted by the Order] assessing the adequacy of management controls for the processing and dissemination of U.S. person information. DIRNSA shall provide the findings of that report to the Attorney General." The Office of the Inspector General (OIG), with the Office of the General Counsel's (OGC) concurrence, issued the aforementioned report on 10 July 2006 in a memorandum with the subject *FISA Court Order: Telephony Business Records (ST-06-0018)*. Subsequently, DIRNSA sent the memorandum to the Attorney General. This report provides the details of our assessment of management controls that was reported to DIRNSA and makes formal recommendations to Agency management.

## FINDING

***~~(TS//SI//[redacted]//OC,NF)~~ The management controls designed by the Agency to govern the processing, dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order are adequate and in several aspects exceed the terms of the Order. Due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, three additional controls should be put in place. Specifically, Agency management should:***

***(1) design procedures to provide a higher level of assurance that non-compliant data will not be collected and, if inadvertently collected, will be swiftly expunged and not made available for analysis.***

***(2) separate the authority to approve metadata queries from the capability to conduct queries of metadata under the Order.***

***(3) conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made under the Order.***

## (U) Criteria

~~(TS//SI/[redacted]~~/OC,NF) **The Order.** The Order authorizes NSA to collect and retain telephony metadata to protect against international terrorism and to process and disseminate this data regarding [redacted] in the United States. To protect U.S. privacy rights, the Order states specific terms and restrictions regarding the collection, processing, retention,[1] dissemination, data security, and oversight of telephony metadata and U.S. person information obtained under the Order. To ensure compliance with these terms and restrictions, the Order also mandates Agency management to implement a series of procedures to control the access to and use of the archived data collected pursuant to the Order. These control procedures are clearly stated in the Order. Appendix B includes a summary of the key terms of the Order and the related mandated control procedures.

(U) **Standards of Internal Control.** Internal control, or management control, comprises the plans, methods, and procedures used to meet missions, goals, and objectives. It provides reasonable assurance that an entity is effective and efficient in its operations, reliable in its reporting, and compliant with applicable laws and regulations. The General Accounting Office's *Standards for Internal Control in the Federal Government*, November 1999 (the Standards), presents the standards that define the minimum level of quality acceptable for management control in government. NSA/CSS Policy 7-3, *Internal Control Program*, advises that evaluations of internal control should consider the requirements outlined by the Standards. The OIG uses the Standards as the basis against which management control is evaluated.

## ~~(TS//SI//NF)~~ Documented Procedures are Needed to Govern the Collection of Telephony Metadata

~~(TS//SI//NF)~~ Control procedures for collecting telephony metadata under the Order were not formally designed and are not clearly documented. As a result, management controls do not provide reasonable assurance that NSA will comply with the following terms of the Order:

[1] ~~(TS//SI)~~ We did not assess the controls over retention at this time as the Order allows data to be retained for five years.

NSA may obtain telephony metadata, which includes comprehensive communications, routing information, including but not limited to session identifying information, trunk identifier, and time and duration of a call. Telephony metadata does not include the substantive content of any communications, or the name, address, or financial information of a subscriber or customer.

~~(TS//SI//NF)~~ As required by the Order, OGC plans to examine periodically a sample of call detail records to ensure NSA is receiving only data authorized by the court. (This is the only control procedure related to collection that is mandated by the Order.) Although this will detect unauthorized data that has been loaded into the archived database, there should also be controls in place to prevent unauthorized data from being loaded into the database. In addition, good internal control practices require that documentation of internal control appear in management directives, administrative policies, or operating manuals. At a minimum, procedures should be established to:

- monitor incoming data on a regular basis,
- upon discovery of unauthorized data, suppress unauthorized data from analysts' view, and
- eliminate unauthorized data from the incoming data stream.

~~(TS//SI//[redacted]/NF)~~ With these proposed control procedures in place, the risk that Agency personnel will mistakenly collect types of data that are not authorized under the Order will be minimized. Although the primary and secondary orders prohibit the providers from passing specific types of data to NSA, mistakes are possible. For example, in responding to our request for information, Agency management discovered that NSA was obtaining two types of data that may have been in violation of the Order: a 16-digit credit card number and name/partial name in the record of Operator-assisted calls. (It should be noted that the name/partial name was not the name of the subscriber from the provider's records; rather, a telephone operator entered name at the time of an Operator-assisted call.)

~~(TS//SI//[redacted]/NF)~~ In the case of the credit card number, OGC advised that, in its opinion, collecting this data is not what the Court sought to prohibit in the Order; but recommended that it still be suppressed on the incoming data flow if not needed for contact chaining purposes. In the case of the name or partial name, OGC advised that, while not what it believed the Court was concerned about when it issued the Order, collecting this information was not in keeping with the Order's specific terms and that it should also be suppressed from the incoming data flow. OGC indicated that it will report these issues to the Court when it seeks renewal of the authorization. Agency management noted that these data types were

blocked from the analysts' view. Management also stated that it will take immediate steps to suppress the data from the incoming data flow. These steps should be completed by July 31, 2006.

**Recommendation 1**

**~~(TS//SI)~~ Design and document procedures to provide a higher level of assurance that non-compliant data will not be collected and, if inadvertently collected, will be swiftly expunged and not made available for analysis.**

**(ACTION: Chief, [redacted])**

***(U) Management Response***

**CONCUR.** ~~(TS//SI//[redacted]//NF)~~ Management concurred with the finding and recommendation and has already partially implemented the recommended procedures to block the questionable data from the providers' incoming dataflow. A final system upgrade to block the questionable data from one remaining provider is scheduled for 8 September 2006. Testing is currently ongoing.

Status: **OPEN**
Target Completion Date: **8 September 2006**

***(U) OIG Comment***

(U) Planned action meets the intent of the recommendation.

## ~~(TS//SI//NF)~~ Additional Controls are Needed to Govern the Processing of Telephony Metadata

~~(TS//SI//NF)~~ Agency management designed, and in some ways exceeded, the series of control procedures over the processing of telephony metadata that were mandated by the Order; however, there are currently no means to prevent an individual who is authorized access the telephony metadata from querying, either by error or intent, a telephone number that is not compliant with the Order. Therefore, additional controls are needed to reduce the risk of unauthorized processing.

~~(TS//SI//[redacted]//OC,NF)~~ Processing refers to the querying, search, and analysis of telephony metadata. To protect the privacy of U.S. persons, the Order restricts the telephone numbers that may be queried:

Based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted]

A telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution.

~~(TS//SI//NF)~~ Agency management designed the series of control procedures over the processing of telephony metadata that were mandated by the Order. In a short amount of time, Agency management modified existing systems and designed new processes to:

- document justifications for querying a particular telephone number,
- obtain and document OGC and other authorized approvals to query a particular telephone number, and
- maintain automatic audit logs of all queries of the telephony metadata.

~~(TS//SI//NF)~~ These controls are adequate to provide reasonable assurance that justifications are sound, approvals are given and documented, and that there is a record of all queries made. Agency management even exceeded the intent of the Order by fully documenting the newly developed processes in Standard Operating Procedures and by developing enhanced logging capability that will, once completed, generate additional reports that are more usable for audit purposes.

~~(TS//SI//NF)~~ Two additional control procedures are needed to provide reasonable assurance that only telephone numbers that meet the terms of the Order are queried.

***~~(TS//SI//NF)~~ The authority to approve metadata queries should be segregated from the capability to conduct metadata queries.***

~~(TS//SI//NF)~~ The Chief and Deputy Chief of the Advanced Analysis Division (AAD) and five Shift Coordinators[2] each have both the authority to approve the querying of telephone numbers under the Order and the capability to conduct queries. The Standards of

[2] ~~(TS//SI//NF)~~ The Order grants approval authority to seven individuals: the SID Program Manager for CT Special Projects, the Chief and Deputy Chief of the AAD, and four Shift Coordinators in AAD. In practice, Agency management transferred the authority of the SID Program Manager for CT Special Projects to one additional Shift Coordinator. Approval authority therefore remains limited to seven individuals as intended by the Order.

Internal Control in the Federal Government require that key duties and responsibilities be divided among different people to reduce the risk of error or fraud. In particular, responsibilities for authorizing transactions should be separate from processing and recording them. This lack of segregation of duties increases the risk that Shift Coordinators and the Chief and Deputy Chief of AAD will approve and query, either by error or intent, telephone numbers that do not meet the terms of the Order.

**Recommendation 2**

**~~(TS//SI)~~ Separate the authority to approve metadata queries from the capability to conduct queries of metadata under the Order.**

**(ACTION: Chief, Advanced Analysis Division)**

### *(U) Management Response*

**CONCUR.** ~~(TS//SI//[redacted]/NF)~~ Management concurred with the finding but stated that it could not implement the recommendation because of constraints in manpower and analytic expertise. As an alternative, management recommended that SID Oversight & Compliance (O&C) routinely review the audit logs of the Chief and Deputy Chief of the Advanced Analysis Division and Shift Coordinators to verify that their queries comply with the Order. This alternative would be developed in conjunction with actions taken to address Recommendation 3 and is contingent on the approval of a pending request to SID management to detail two computer programmers to the team. Management is also negotiating with O&C to accept the responsibility for conducting the recommended reconciliations.

Status: **OPEN**
Target Completion Date: **28 February 2007**

### *(U) OIG Comment*

~~(TS//SI//[redacted]/NF)~~ Although not ideal, management's alternative recommendation to monitor audit logs to detect errors will, at a minimum, mitigate the risk of querying telephone numbers that do not meet the terms of the Order. Therefore, given the existing manpower constraints, management's suggested alternative recommendation meets the intent of the recommendation.

~~(TS//SI//NF)~~ *Audit logs should be routinely reconciled to the records of telephone numbers approved for querying.*

~~(TS//SI//NF)~~ Management controls are not in place to verify that those telephone numbers approved for querying pursuant to the Order are the only numbers queried. Although audit logs document all queries of the archived metadata as mandated by the Order, the logs are not currently generated in a usable format, and Agency management does not routinely use those logs to audit the telephone numbers queried. The Standards of Internal Control in the Federal Government recommends ongoing reconciliations to "make management aware of inaccuracies or exceptions that could indicate internal control problems." The lack of routine reconciliation procedures increases the risk that errors will go undetected.

**Recommendation 3**

**~~(TS//SI)~~ Conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made under the Order.**

**(ACTION: SID Special Program Manager for CT Special Projects)**

*(U) Management Response*

**CONCUR.** ~~(TS//SI//[redacted]//NF)~~ Management concurred with the finding and recommendation and presented a plan to develop the necessary tools and procedures to implement the recommendation. However, management stated that completion of the planned actions is contingent on the approval of a pending request to SID management to detail two computer programmers to the team. Management is also negotiating with O&C to accept the responsibility for conducting the recommended reconciliations.

Status: **OPEN**
Target Completion Date: **28 February 2007**

*(U) OIG Comment*

(U) Planned action meets the intent of the recommendation. However, should SID management not grant the request for additional computer programmers or O&C not accept responsibility for conducting the reconciliations, management must promptly inform the OIG and present an alternative plan.

**Observation**

*(TS//SI//NF) At the time of our review, there was no policy in place to periodically review telephone numbers approved for querying under the Order to ensure that the telephone numbers still met the criteria of the Order. Although the Order is silent on the length of time a telephone number may be queried once approved, due diligence requires that Agency management issue a policy decision on this matter and develop procedures to execute the decision.*

## ~~(TS//SI//NF)~~ Management Controls Governing the Dissemination of U.S. Person Information are Adequate

~~(TS//SI//NF)~~ Agency management implemented the series of control procedures governing the dissemination of U.S. person information mandated by the Order. O&C designs and implements controls to ensure USSID SP0018 compliance across the Agency, to include obtaining the approval of the Chief of Information Sharing Services and maintaining records of dissemination approvals, as required by the Order. No additional procedures are needed to meet the intent of the Order. Furthermore, these procedures are adequate to provide reasonable assurance that the following terms of the Order are met:

> Dissemination of U.S. person information shall follow the standard NSA minimization procedures found in the Attorney General-approved guidelines (USSID 18).

## ~~(TS//SI//NF)~~ Management Controls Governing Data Security are Adequate

~~(TS//SI//NF)~~ Agency management implemented the series of control procedures governing the data security of U.S. person information as mandated by the Order, such as the use of user IDs and passwords. Agency management exceeded the terms of the Order by maintaining additional control procedures that provide an even higher level of assurance that access to telephony metadata will be limited to authorized analysts. Most of these controls had been in place prior to and aside from the issuance of the Order. Only the requirement that OGC periodically monitor individuals with access to the archive was designed in response to the Order. Combined, these procedures are adequate to provide reasonable assurance that Agency management complies with the following terms of the Order:

> DIRNSA shall establish mandatory procedures strictly to control access to and use of the archived metadata collected pursuant to this Order.

~~(TS//SI//NF)~~ Additionally, O&C plans to reconcile the list of approved analysts with a list of authorized users to ensure only approved analysts have access to the metadata.

## ~~(TS//SI//NF)~~ Management Controls Governing the Oversight of Activities Conducted Pursuant to the Order are Adequate

~~(TS//SI//NF)~~ As mandated by the Order, Agency management designed plans to provide general oversight of activities conducted pursuant to the Order. The Order states that,

> The NSA Inspector General, the NSA General Counsel, and the Signals Intelligence Directorate Oversight and Compliance Office shall periodically review this program.

~~(TS//SI/[redacted]/OC,NF)~~ Specifically, Agency management designed the following plans that are adequate to ensure compliance with the Order.

- ~~(TS//SI//NF) The~~ OGC will report on the operations of the program for each renewal of the Order.
- ~~(TS//SI//NF) O~~&C plans to conduct periodic audits of the queries.
- ~~(TS//SI//NF)~~ OIG planned to audit telephony metadata [redacted] Upon issuance of the Order, the audit was put on hold to complete the court-ordered report. OIG will modify the audit plan to include the new requirements of the Order. Once sufficient operations have occurred under the Order to allow for a full range of compliance and/or substantive testing, the audit will proceed.

## (U) Conclusion

~~(TS//SI//NF)~~ The activities conducted under the Order are extremely sensitive given the risk of encountering U.S. person information. The Agency must take this responsibility seriously and show good faith in its execution. Much of the foundation for a strong control system is set up by the Order itself, in the form of mandated control procedures. In many ways, Agency management has made the controls even stronger. Our recommendations will address control weaknesses not covered by the Order or Agency management and will meet Federal standards for internal control. Once the noted weaknesses are addressed, and additional controls are implemented, the management control system will provide reasonable assurance that the terms of the Order will not be violated.

# APPENDIX A

## (U) About the Audit

This page intentionally left blank

# (U) ABOUT THE AUDIT

## (U) Objectives

~~(TS//SI)~~ The overall objective of this review was to determine whether management controls will provide reasonable assurance that Agency management complies with the terms of the Order. Specific objectives were to:

- verify that Agency management has designed the control procedures mandated by the Order.
- assess the adequacy of all management controls in accordance with the *Standards of Internal Control in the Federal Government*.

## (U) Scope and Methodology

~~(U//FOUO)~~ The audit was conducted from May 24, 2006 to July 8, 2006.

~~(U//FOUO)~~ We interviewed Agency personnel and reviewed documentation to satisfy the review objectives.

~~(TS//SI)~~ We did not conduct a full range of compliance and/or substantive testing that would allow us to draw conclusions on the efficacy of management controls. Our assessment was limited to the overall adequacy of management controls, as directed by the Order.

~~(TS//SI)~~ As footnoted, we did not assess controls related to the retention of telephony metadata pursuant to the Order. As the Order authorizes NSA to retain data for up to five years, such controls would not be applicable at this time.

This page intentionally left blank

# Appendix B

## ~~(U//FOUO)~~ Telephony Business Records FISC Order - Mandated Terms and Control Procedures

This page intentionally left blank

# (U) Business Records FISC Order

## (U) Mandated Terms and Control Procedures

~~(TS//SI//NF)~~

| Control Area | Terms of the Order | Responsible Entity | Control Procedures |
|---|---|---|---|
| Collection of Metadata | NSA may obtain telephony metadata, which includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, communications device identifier, etc.), trunk identifier, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 USC 2510(8) or the name, address, or financial information of a subscriber or customer (pg. 2, para 2). | OGC | At least twice every 90 days, OGC shall conduct random spot checks, consisting of an examination of a sample of call detail records obtained, to ensure that NSA is receiving only data as authorized by the Court and not receiving the substantive content of the communications (pg. 10, para (4)J). |

~~(TS//SI//NF)~~

| Control Area | Terms of the Order | Responsible Entity | Control Procedures |
|---|---|---|---|
| Processing<br><br>(Search & Analysis, or Querying of Archived Metadata) | Although data collected under this order will be broad, the use of that information for analysis shall be strictly tailored to identifying terrorist communications and shall occur solely according to the procedures described in the application (pg. 6, para (4)D). | OGC | OGC shall review and approve proposed queries of archived metadata based on seed account numbers reasonably believed to be used by U.S. persons (pg. 6, para (4)C). |
| | Any search or analysis of the data archive shall occur only after a particular known telephone number has been associated with [redacted] (pg. 5, para (4)A). | PM, Chief or D/Chief of AAD, Shift Coordinators | Queries of archived data must be approved by one of seven persons: SID PM for CT Special Projects, the Chief or Deputy Chief, Counterterrorism Advanced Analysis Division, or one of the four specially authorized CT Advanced Analysis Shift Coordinators in the Analysis and Production Directorate of SID (pg. 7, para (4)D). |
| | ▪ Based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted] (pg. 5, para (4)A); | PM; Chief & D/Chief of AAD, & Shift Coordinators | SID PM for CT Special Projects; Chief and Deputy Chief, CT Advanced Analysis Division, and CT Advanced Analysis Shift Coordinators shall establish appropriate management controls (e.g., records of all tasking decisions, audit and review procedures) for access to the archived data (pg. 8, para (4)G). |
| | | AAD Analysts | *Maintain a record of justifications because* at least every ninety days, the Department of Justice shall review a sample of NSA's justifications for querying the archived data (pg. 8, para (4)E). |
| | ▪ A telephone number believed to be used by a U.S. person shall not be regarded as associated with [redacted] solely on the basis of activities that are protected by the First Amendment to the Constitution (pg. 5, para (4)A). | [redacted] and Technical Support | When the metadata archive is accessed, the user's login, IP address, date and time, and retrieval request shall be automatically logged for auditing capability (pg. 6, para (4)C).<br><br>OGC will monitor the functioning of this automatic logging capability (pg. 6, para (4)C). |
| | DIRNSA shall establish mandatory procedures strictly to control access to and use of the archived data collected pursuant to this Order (pg. 5, para (4)A). | OGC<br><br>OGC | Analysts shall be briefed by OGC concerning the authorization granted by this Order and the limited circumstances in which queries to the archive are permitted, as well as other procedures and restrictions regarding the retrieval, storage, and dissemination of the archived data (pg. 6, para (4)G). |

~~(TS//SI//NF)~~

| Control Area | Terms of the Order | Responsible Entity | Control Procedures |
|---|---|---|---|
| Dissemination of U.S. Person Information | Dissemination of U.S. person information shall follow the standard NSA minimization procedures found in the Attorney General-approved guidelines (USSID 18) (pgs. 6-7, para (4)D) & pg. 8, para (4)G). | Chief of Information Sharing Services in SID | Prior to the dissemination of any U.S. person identifying information, the Chief of Information Sharing Services in SID must determine that the information identifying the U.S. person is in fact related to Counterterrorism information and that it is necessary to understand the Counterterrorism information or assess its importance (pg. 7, para (4)D).<br>A record shall be made of every such determination (pg. 7, para (4)D). |
| Metadata Retention | Metadata collected under this Order may be kept online (that is, accessible for queries by cleared analysts) for five years, at which time it shall be destroyed (pg. 8, para (4)F). | [redacted] and Technical Support | None |
| Data Security | (TS//SI//NF) DIRNSA shall establish mandatory procedures strictly to control access to and use of the archived data collected pursuant to this Order (pg. 5, para (4)A). | [redacted] and Technical Support<br><br>OGC | The metadata shall be stored and processed on a secure private network that NSA exclusively will operate (pg. 5, para (4)B).<br>Access to the metadata archive shall be accomplished through a software interface that will limit access to this data to authorized analysts controlled by user name and password (pg. 5, para (4)C).<br>OGC shall monitor the designation of individuals with access to the archive (pgs. 5-6, para (4)C). |
| Oversight | The IG, GC, and the SID Oversight and Compliance Office shall periodically review this program (pg. 8, para (4)H). | IG, GC, and SID Oversight and Compliance Office<br><br>DIRNSA | The IG and GC shall submit a report to DIRNSA 45 days after the initiation of the activity assessing the adequacy of the management controls for the processing and dissemination of U.S. person information (pg. 8, para (4)H).<br>DIRNSA shall provide the findings of that report to the Attorney General (pg. 9, para (4)H). |

This page intentionally left blank

# Appendix C

## ~~(U//FOUO)~~ Full Text of Management Comments

This page intentionally left blank

PROGRAM MEMORANDUM

PM-031-06 Reissued
29 Aug 2006

To: Office of the Inspector General [redacted]

Cc: Office of [redacted]
Counterterrorism Production Center [redacted]
Chief, SID Oversight and Compliance [redacted]
SSG1 [redacted]

SUBJECT: ~~(TS//SI//NF)~~ PMO Response to IG-10681-06, Subject Draft Report on the Assessment of Management Controls for implementing the FISA Court Order: Telephony Business Records (ST-06-0018)

1. ~~(U//FOUO)~~ The SIGINT Directorate Program Office appreciates and welcomes the Inspector General Office's review of program operations as required by the subject court order. The Program Office offers the following response.

2. ~~(TS//SI//NF)~~ This report presents three findings/recommendations. Finding one pertains to procedures to provide a higher level of assurance that non-compliant data will not be collected and, if inadvertently collected, will be swiftly expunged and not made available for analysis. Finding two pertains to the goal to separate the authority to approve metadata queries from the capability to conduct queries. Finding three pertains to the requirement to conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made.

3. ~~(TS//SI//[redacted]//NF)~~ With respect to Finding One, the Program Office acknowledges that the item is factually correct and concurs with the assessment with comment. It should be noted that internal management controls, known as software rules that are part of the [redacted] database, do prevent the data in question from ever being loaded into the operational contact chaining databases. Still, the data in question did exist in the dataflow and should be suppressed on the provider-end as the OIG recommends.

a. ~~(TS//SI//[redacted]//NF)~~ Corrective Actions: Although already partially implemented among the providers, the final system upgrade necessary to block the data in question from one provider on the incoming dataflow is scheduled to be in place by 8 September 2006. Testing continues at this time.

4. ~~(TS//SI//NF)~~ Finding Two recommends two additional controls. With respect to the first, "The authority to approve metadata queries should be segregated from the capability to conduct metadata queries", the Program Office agrees the assessment has merit, but cannot implement the required corrective actions. In theory, the OIG recommendation is sound and conforms fully to the standards of internal control in the Federal Government. In practical terms, it is not something that can be easily implemented given the

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20041123~~
~~Declassify On: 20301115~~

risk/benefit tradeoff and real world constraints. Manpower ceilings and available analytic expertise are the two most significant limiting factors.

5. ~~(TS//SI//NF)~~ The Advanced Analysis Division (S2I5) is comprised of personnel of varying grades and experience levels. Given the requirements of the court order, the Shift Coordinators are required to be the most experienced intelligence analysts, have the most training and consequently hold the most senior grade levels. They therefore are given the authority to approve data queries, and because of their status can also execute queries. Removing this dimension of their authorities would severely limit the versatility of the most experienced operations personnel. Also, as their title implies, they are also the most senior personnel present during each operational shift and in effect control the ops tempo on the operations floor. Replicating that senior structure to accommodate the OIG recommendation is not possible given current manning authorizations and ops tempo.

a. ~~(TS//SI//NF)~~ However, there are checks and balances already in place to help mitigate the risks cited. For example, the Shift Coordinators routinely approve queries into the database based on selectors meeting a reasonable articulable suspicion standard IAW with NSA OGC written guidelines and verbal briefings. Any queries initiated from probable U.S. selectors must be individually approved by the OGC. In this way, the risk of error or fraud associated with the requirements of the court order is acceptably mitigated within available manning and analytic talent constraints.

b. ~~(TS//SI//NF)~~ Corrective Actions: Corrective actions cannot be implemented without significantly increasing manning levels of senior, highly skilled analysts. In our view, the benefit gained will not justify the manpower increase required. However, it may be possible to implement additional checks and audits on the query approval process. As recommended in the response to Finding Three below, Oversight and Compliance could, if they accept an expanded role, use (yet to be developed) new automated software tools to regularly review the audit logs of all shift coordinators. With software changes to the audit logs it would be possible to easily compare numbers approved and their accompanying justifications against numbers chained. In this way, it would be possible to review the shift coordinator's actions against the standards established by the court. The Program Office recommends that this corrective action be pursued as part of the long term goal discussed below.

6. ~~(TS//SI//NF)~~ Finding Three reads "conduct periodic reconciliation of approved telephone numbers with the logs of queried numbers to verify that only authorized queries have been made under the order". The Program Office agrees with this assessment. However, competing priorities for the software programming talent necessary to implement improvements to the audit logs, as well as to perform the programming necessary to create automated reconciliation reports, require that this issue be addressed as a long term goal.

a. ~~(TS//SI//NF)~~ If SID management approves a pending Program Office request to detail two computer programmers to the team for six-to-nine month rotations, suitable procedures and software tools could be implemented. Also, the Program Office has approached the office of Oversight and Compliance about accepting the responsibility of conducting the recommended audits. That negotiation is ongoing.

b. ~~(TS//SI//NF)~~ Corrective Action: Acceptable tools and procedures can be developed within six months if the required manpower is allocated. Assuming the Program team's request is granted, this initiative can be completed by 28 February 2007. The corrective action will include:

1. ~~(U//FOUO)~~ Improvements to the audit logs to make them more user friendly

2. ~~(U//FOUO)~~ Reports that provide a useable audit trail from requester, to approver, to any resulting reports. These reports will be used to automatically identify any discrepancies in the query process (i.e. queries made, but not approved).

3. ~~(U//FOUO)~~ Complete the negotiations with SID Oversight & Compliance

7. ~~(U//FOUO)~~ Please contact me if you have additional questions.

[redacted]

29 Aug 06

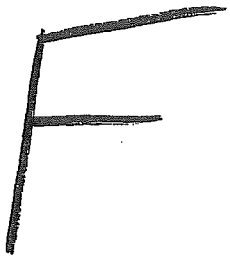
SID Program Manager
CT Special Programs

# IT'S EVERYBODY'S BUSINESS –

TO REPORT SUSPECTED INSTANCES OF FRAUD,
WASTE, AND MISMANAGEMENT, CALL OR VISIT
THE NSA/CSS IG DUTY OFFICER
ON 963-5023s/[redacted]
IN OPS2A/ROOM 2A0930

IF YOU WISH TO CONTACT THE OIG BY MAIL,
ADDRESS CORRESPONDENCE TO:

DEPARTMENT OF DEFENSE
NATIONAL SECURITY AGENCY/
CENTRAL SECURITY SERVICE
ATT: INSPECTOR GENERAL
9800 SAVAGE ROAD, STE 6247
FT. MEADE, MD 20755-6247



**OFFICE OF THE INSPECTOR GENERAL**
**NATIONAL SECURITY AGENCY**
**CENTRAL SECURITY SERVICE**

10 July 2006
IG-10667-06

TO: DIRECTOR, NSA

SUBJECT: ~~(TS//SI//NF)~~ FISA Court Order: Telephony Business Records (ST-06-0018)

1. ~~(TS//SI//NF)~~ **Background and Objective.** The Order of the Foreign Intelligence Surveillance Court issued 24 May 2006 in *In Re Application of the FBI etc.*, No. BR-06-05 (Telephony Business Records) states that "[t]he Inspector General and the General Counsel shall submit a report to the Director of NSA 45 days after the initiation of the activity [permitted by the Order] assessing the adequacy of the management controls for the processing and dissemination of U.S. person information." This is that report. The Order further states that "[t]he Director of NSA shall provide the findings of that report to the Attorney General." Order at 8-9. The Order sets no deadline for transmission of the findings to the Attorney General.

2. ~~(TS//SI//NF)~~ **Finding.** The management controls designed by the Agency to govern the processing, dissemination, security, and oversight of telephony metadata and U.S. person information obtained under the Order are adequate and in several aspects exceed the terms of the Order. However, due to the risk associated with the collection and processing of telephony metadata involving U.S. person information, three additional controls should be put in place. Specifically, Agency management should (1) design procedures to provide a higher level of assurance that non-compliant data will not be collected and, if inadvertently collected, will be swiftly expunged and not made available for analysis; (2) separate the authority to approve metadata queries from the capability to conduct queries of metadata under the Order; and (3) conduct periodic reconciliation of approved telephone numbers to the logs of queried numbers to verify that only authorized queries have been made under the Order.

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20041123~~
~~Declassify On: MR~~

3. (~~TS//SI~~) **Further Review.** The Inspector General will make formal recommendations to the Director, NSA/CSS, in a separate report regarding the design and implementation of the additional controls.

4. (U//~~FOUO~~) We appreciate the courtesy and cooperation extended throughout our review to the auditors from the Office of the Inspector General and the attorneys from the Office of the General Counsel who consulted with them. If you need clarification or additional information please contact [redacted] on 963-1421(s) or via e-mail at [redacted]

JOEL F. BRENNER
Inspector General

(U//~~FOUO~~) I endorse the conclusion that the management controls for the processing and dissemination of U.S. person information are adequate.

ROBERT L. DEITZ
General Counsel

DISTRIBUTION:

SIGINT Director
SID Program Manager for CT Special Projects
Chief, S2
Chief, S2I
Chief, S2I5
Chief, S3
Chief, S33
OGC
SID O&C

G

**FM: SID Oversight & Compliance**

**Date: 11 July 2006**

**Subject: Final Responses to the OIG – Request for Information - Business Records Order (U)**

SID Oversight and Compliance

1. **~~(TS//SI//NF)~~ Written plans for periodically reviewing this program.**

~~(TS//SI//NF)~~ SID Oversight and Compliance will:

- In coordination with Program Office, conduct weekly reviews of list of analysts authorized to access Business Records data and ensure that only approved analysts have access. Oversight & Compliance will inform NSA's Office of General Counsel (OGC)of the results of the reviews and provide copies if needed to OGC.
- Perform periodic super audits of queries.
- Work with the Program Office to ensure that the data remains appropriately labeled, stored and segregated according to the terms of the court order.

2. **~~(TS//SI//NF)~~ Written procedures in addition to USSID SP0018 to ensure compliance with standard NSA minimization procedures for the dissemination of U.S. person information.**

~~(TS//SI//NF)~~ SID Oversight and Compliance has a documented SOP which outlines the process to ensure compliance with standard NSA minimization procedures:

- During normal duty hours, every report from this order containing U.S. or 2nd Party identities is reviewed by SID Oversight and Compliance prior to dissemination.
- SID Oversight & Compliance (SV) reviews the products (Tippers) and creates a "one-time dissemination" authorization memorandum for signature of the Chief or Deputy Chief of Information Sharing Services.
- The NSOC SOO approves dissemination authorizations after hours.
- S2I/Counterterrorism Production Center provides SV with a copy of any report that is approved by NSOC/SOO for dissemination.
- Oversight and Compliance then issues a memorandum for the record stipulating that the U.S. or 2nd Party identities contained in that report were authorized for dissemination by the NSOC/SOO.

~~Derived From: NSA/CSSM 1-52~~
~~Dated: 20041123~~
Declassify On: 20301129